Владимирский государственный университет

А. М. ЮДИНА

ОСНОВЫ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ (КИБЕРСРЕДА) В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие

Владимир 2025

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»

А. М. ЮДИНА

ОСНОВЫ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ (КИБЕРСРЕДА) В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие

Электронное издание

Владимир 2025

ISBN 978-5-9984-1982-9

УДК 004.056:37.014
ББК 16.8+74.04

Рецензенты:
Доктор педагогических наук, профессор
профессор кафедры оперативно-розыскной деятельности
Юридического факультета Владимирского юридического института
Федеральной службы исполнения наказаний
О. М. Овчинников

Доктор педагогических наук, кандидат юридических наук,
профессор, заслуженный работник высшей школы Российской Федерации
профессор кафедры психологии личности и специальной педагогики
Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
Л. К. Фортова

Издается по решению редакционно-издательского совета ВлГУ

Юдина, А. М.

Основы нормативно-правового регулирования информационных отношений (киберсреда) в образовательной деятельности [Электронный ресурс] : учеб. пособие / А. М. Юдина ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2025. – 176 с. – ISBN 978-5-9984-1982-9. – Электрон. дан. (1,97 Мб). – 1 электрон. опт. диск (CD-ROM). – Систем. требования: Intel от 1,3 ГГц ; Windows XP/7/8/10 ; Adobe Reader ; дисковод CD-ROM. – Загл. с титул. экрана.

Рассмотрены теоретико-методологические проблемы исследования нормативно-правового регулирования информационных отношений (киберсреда) в образовательной деятельности, раскрыты роль информационно-коммуникативной культуры в развитии современного российского общества и возможности социокультурной толерантности как одного из подходов к исследованию коммуникативной культуры студентов и профилактике терроризма. Проанализированы проблемы и перспективы киберсоциализации относительно правовой, информационно-коммуникативной культуры студентов и обоснована инновационная триада педагогических подходов в педагогическом проектировании ценностей и смыслов для централизованной профилактики терроризма.

Предназначено для студентов направлений подготовки 44.03.05, 44.03.01, 44.04.01 «Педагогическое образование». Может быть полезно специалистам, интересующимся проблемами современной киберсоциализации, профилактикой терроризма и неонацизма.

Рекомендовано для формирования профессиональных компетенций в соответствии с ФГОС ВО.

Библиогр.: 36 назв.

ISBN 978-5-9984-1982-9

ОГЛАВЛЕНИЕ

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

ВВЕДЕНИЕ

В условиях роста влияния цифровых технологий на мировое пространство наблюдается заметное увеличение трансформаций традиционных форм – социальных, экономических, технологических и политических феноменов. Такая ситуация приводит к тому, что стихийно формируются новые симулякры, явления, факты, которые нуждаются в правовом осмыслении и анализе. Новые телекоммуникационные технологии, искусственный интеллект, трансграничная цифровизация значимых социально-экономических секторов деятельности, характерные для SHIVA-, TACI-моделей, с 2023 года выступают константами новой постгуманистической реальности.

Социально-экономические отношения, безусловно, не изменили своего вектора, но получили новые возможности определения формы цифровых трансформационных процессов. Государственное регулирование вынуждено реагировать на стремительный прогресс инновационных технологий, кибернетики, искусственного интеллекта (ИИ), дополненной реальности (AR), виртуальной реальности (VR) и обратно пропорциональный процесс снижения информационно-коммуникативной культуры в социальной среде. Это обусловлено повышением возможностей для любого пользователя без специальных знаний получить доступ к глобальному пространству, содержащему, например, многофункциональные базы данных разных государств.

Хакерские террористические атаки, кибермошенничество, киберпреступность, активное участие в киберсреде 99 % молодежи, трансграничный бизнес, выход фондовых рынков, применение блокчейн-технологий в организации голосования в киберсети сосуществуют одновременно, поскольку сеть Интернет лишена нормативно-правового регулирования не только в России, но и во всем мировом пространстве.

Законодатель сегодня вынужден адаптироваться к ежедневно появляющимся формам цифровых взаимодействий между разными участниками отношений в сфере применения кибертехнологий и киберинформационной среды. Разработанная в Российской Федерации

Стратегия развития информационного общества на 2017 – 2030 годы определяет наиболее важные принципы этих процессов. Заслуживает внимания деятельность законодателя, направленная на разработку и создание информационной инфраструктуры, которая позволит гражданам, органам государственной власти, транснациональным корпорациям беспрепятственно получать доступ к открытому Интернету, имея полную «свободу выбора получения знаний при работе с информацией», а значит, и свободу технологической инфраструктуры. В то же время интересны идеи о приоритете традиционных ценностей над киберсемиотикой, инициации преобладания традиционных норм, правил, коммуникаций в киберотношениях, упорядочивании распространения информации о юридических и физических лицах. Важная задача государства и институтов гражданского общества – создание информационной безопасности в киберсреде в условиях глобализации.

Правовое регулирование информационных отношений в киберсреде подразумевает условное деление круга источников на группы: правовые источники (акты законодательства и подзаконные акты); доктринальные источники (исследования ученых-юристов); правоприменительные источники (анализ положительной и отрицательной практики применения законодательства, статистических источников (социологические исследования: отчеты о работе ООН, ЕС ОЭС)).

В приложении приведена рабочая программа дисциплины «Нормативно-правовые основы образовательной деятельности».

Глава 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЩЕСТВЕННЫХ ОТНОШЕНИЙ В СФЕРЕ КИБЕРСРЕДЫ (В КОНТЕКСТЕ ГЛОБАЛИЗАЦИИ)

1.1. Характеристика киберпространства в условиях глобализации

В условиях глобализации чрезвычайно важное значение имеют вопросы методологического характера исследования правового регулирования социальных взаимодействий в киберсреде. Для более четкого осмысления поставленной проблемы необходимо определить методы правового регулирования и его значение для раскрытия основополагающих свойств информационно-коммуникативной среды в современных реалиях.

Автор разделяет точку зрения исследователя М. Н. Марченко, который постулировал, что к настоящему времени нет полной ясности в определении концептуальных основ категории «право». Оно до сих пор употребляется в объективном и субъективном значениях. Нельзя не согласиться с правоведами в том, что право – это пока что нерешенная проблема.

Что же означает категория «право» применительно к киберпространству в условиях глобализации? Это конгломерат тех правовых положений, которые отражены в нормативно-правовых актах, регулирующих сферу использования информационной инфраструктуры, а также симбиоз принципов, отражающих состояние правотворчества и правосознания как источников формирования поведенческой стратегии личности в киберпространстве.

С точки зрения Д. А. Керимова, по отношению к киберпространству законодательство не вправе копировать общественные отношения. Оно должно инициировать субъективную деятельность законодателя, участвующего в законодательном установлении[1].

Регулирование правовой нормы в сфере киберпространства коррелирует с мировоззрением законодателя. Следовательно, от его профессионализма, скрупулезности и ответственности зависит регуляция информационной инфраструктуры.

---

[1] Керимов Д. А. Методология права. Предмет, функции, проблемы философии права. 3-е изд., перераб. и доп. М. : Норма : ИНФРА-М, 2020. С. 103.

Важно определить тезаурус правового регулирования, используемый при анализе общественных отношений в сфере киберпространства, поскольку это позволит выявить симбиоз признаков и актуализировать новые дефиниции.

В 1996 году 4 октября протоколом № 10 Межгосударственный совет по стандартизации, метрологии и сертификации принял единую методологию стандартизации терминологии[1], по которому необходимо придерживаться требований, применяемых к полученным категориям и дефинициям: адекватность содержания, оперирование только основополагающими признаками, недопустимость тавтологии и негативной дефиниции для термина, отражающего позитивную сущность, неперегрузка термина дополнительными уточнениями и лингвистическая корректность трактовки понятия.

В учебном пособии представлен интегрированный подход к методологии международного и информационного права. Для дальнейшего анализа целесообразно выделить диалектический, семиотический, общенаучный методы и специальные методы международного, образовательного, информационного права в Российской Федерации[2].

Использование диалектического, семиотического методов как инструментов информационного, международного права объясняется тем, что они раскрывают общие закономерности изучаемого феномена, выявляют противоречия, которые заложены в содержании предмета исследования.

Эти методы очень важны, поскольку актуализируют глубину изучения общественных отношений, возникающих в киберпространстве, позволяют проанализировать противоречия между ними, а также дают возможность выявить идентичность и тождественность реального и виртуального миров.

Разделяя концептуальные идеи О. А. Городова[3], можно сделать вывод, что совершенствование категории «информация» было реализовано в кибернетической, смысловой и практической траекториях,

---

[1] Рекомендации по межгосударственной стандартизации (РМГ): РМГ 19-96 // Документы в области метрологии : указатель / Федер. агентство по техн. регулированию и метрологии ; сост.: П. К. Одинцов [и др.]. М. : Стандартинформ, 2020. С. 221.

[2] Бачило И. Л. Информационное право : учеб. для вузов. 5-е изд., перераб. и доп. М. : Юрайт, 2022. С. 73.

[3] Городов О. А. Информационное право : учеб. для бакалавров. 2-е изд., стер. М. : Проспект, 2016. С. 10 – 15.

детерминированных с опорой на категорию «информация» в разнообразных сферах жизненного пространства индивида.

Анализируя семантическую теорию информации, предложенную Ю. А. Шрейдером, можно сделать вывод, что ее квинтэссенцией являются характерологические особенности данного феномена, которые и раскрывают ее семантическое значение[1].

Что же касается специальных методов, применяемых для анализа проблематики информационного права в гносеологическом аспекте, то необходимо учитывать, что они заимствованы из других областей, например из социально-культурной практики. В то же время сегодня постепенно формируются собственные методы информационного права.

Особенно хотелось бы выделить практические методы изучаемого феномена, которые применяются при поиске, хранении и популяризации информации, а также ее оценке.

Общенаучные методы (наблюдение, сравнение, описание) заимствованы из психологии и применяются при исследовании информационных объектов.

Сегодня необходимо постулировать о дифференциации информации с точки зрения информационного права на свободную и связанную[2].

Проблема современного общества, особенно в условиях глобализации, состоит в том, что ежедневно на человека обрушивается огромный поток информации, тогда как ее объем должен коррелировать с теми особенностями окружающего социума, которые раскрывают наиболее значимые процессы и явления.

Информация может быть как объективной, так и субъективной. Человек создает информацию неспонтанно, поскольку изменяется и стратегия его деятельности. XXI век характеризует человекомашинный симбиоз, заключающийся в проникновении технологий внутрь индивида с целью расширения его психосоматических, физических и интеллектуальных способностей. Изменяя деятельность человека, технологии модифицируют и общественные отношения, создавая новые, актуализируя механизмы правового регулирования и идентификацию субъектов в Интернете. Однако кроме позитивных послед-

[1] Шрейдер Ю. А. Социальные аспекты информатики // НТИ. 1989. С. 3 – 14.
[2] Городов О. А. Указ. соч. С. 20 – 23.

ствий технологии имеют и негативные: они усугубляют конфликтные отношения и разжигают информационные войны. Почему это происходит? Распространяя информацию на большие территории, технологии вовлекают в отношения большое количество индивидов, искажая мировоззрение. Сложность состоит в том, что очень четко определить источник информации практически невозможно, поскольку их может быть много и они варьируются: например, для блокирования или трансформации информации в условиях информационной войны (DDoS-атаки), для контроля работы провайдеров и серверов, а также вывода их из рабочего состояния.

Технологии оказали влияние и на распознавание места совершения преступления, на отношения, которые возникли в глобальной сети, и в этой связи категория «территория» перешла в категорию «трансграничность». Такие технологии, как пиринговые сети, блокчейн, tor-протоколы, анонимные сети, представляют собой распределенную сеть, позволяющую применять вычислительные возможности в разных странах для реализации определенных задач.

Изучая основы нормативно-правового регулирования информационных киберотношений, возникающих в образовательной среде, становится закономерным то, что правовое регулирование киберотношений не может идти вровень с развитием технологий, поскольку законы не разрабатываются «на перспективу». Но в образовательной сфере важно учитывать принцип культуросообразности в работе с обучающимися, предполагающий объяснение цифровых норм и правил в сети Интернет, в том числе для профилактики и противодействия кибертеррористической идеологии.

В глобальной сети существуют как конструктивные, так и деструктивные отношения. Интернет оказал существенное влияние на все области деятельности человека, включая взаимодействие индивида с социумом и государством.

В такой ситуации цифровизация трансформирует все социокультурные отношения: сегодня появились инновационные информационные субъекты – информационный хостинг (провайдеры), сетевые издания в режиме реального времени (блоги разных информационных платформ), киберсообщества, IOT, Big Data, криптовалюта и т. д.

При анализе цифровых технологий, обеспечивающих информационную безопасность для личности, социума, государства, необхо-

димо, опираясь на систему права, вести профилактику кибертерроризма, делинквентного поведения молодежи в сети Интернет.

Упомянутая проблема трансграничных трансляций Big Data в киберсреде актуализирует потребность создания единых правил и правовых подходов на международном уровне. В современных реалиях подавляющее число государств регулируют указанные отношения национальным законодательством. Например, 26 октября 2016 года Правительство Российской Федерации приняло постановление № 1101 «О единой автоматизированной информационной системе “Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено”», которое направлено на реализацию блокировки деструктивных ресурсов в Интернете[1].

На современном уровне развития педагогических и правовых наук наблюдается ряд противоречий, возникающих в рамках реальной правоприменительной практики применения информационно-коммуникационной технологии. До сих пор существуют проблемные зоны, указывающие на нестыковки права и современных реалий в киберсреде.

[1] Постановление Правительства Рос. Федерации от 26.10.2012 № 1101 (ред. от 12.10.2021) «О единой автоматизированной информационной системе “Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено"» (вместе с "Правилами создания, формирования и ведения единой автоматизированной информационной системы "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено"», "Правилами принятия уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти решений в отношении отдельных видов информации и материалов, распространяемых посредством информационно-телекоммуникационной сети "Интернет", распространение которых в Российской Федерации запрещено") / Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 14.09.2021).

Сегодня объективно выявлены технологии, опираясь на которые, третьи лица оказывают влияние на работу ряда объектов различных государств, с чем и связана их озабоченность в плане обеспечения международной информационной безопасности.

А. Н. Савенков отметил, что в 2017 году Россия в рейтинге Международного союза электросвязи по индексу кибербезопасности заняла 10-е место, опередив на один пункт такие развитые страны, как Япония и Норвегия[1]. Таким образом, исследователь обращает внимание на неравномерность развития интернет- и кибертехнологий и в технологическом, и в правовом контексте.

Отмеченные платформы блокчейн и криптовалют требуют регулирования общественных отношений. Федеральный закон «О персональных данных» может быть применен при обработке большого количества данных и передаче конгломерата изображений, звука, текста, включая многопользовательские задачи.

Исследователи В. Б. Исаков, В. К. Сарьян, А. А. Фокина конституируют, что технологическая, информационная и soft безопасность информационных систем, включающих критически значимые объекты, актуализирует безотлагательность исследований новых правовых подходов в этой сфере[2].

Сегодня законодатель должен продумать и нормы технического регулирования, согласованные с нормами правового регулирования, поскольку разрушительное программное обеспечение самым негативным образом воздействует на функционирование киберпространства.

Изучая основы нормативно-правового регулирования (информационных отношений) в киберсреде, можно констатировать, что сегодня появляются такие субъекты, как информационные посредники, активно взаимодействующие с государством, инициирующие организацию частно-государственного сотрудничества, но создающие дифференцированные возможности для качественного правового регулирования через инновационные глобальные информационные инфраструктуры (ГИИ).

---

[1] Global Cybersecurity Index (GCI) 2017. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI-17Report.pdf (дата обращения: 14.09.2024).

[2] Исаков В. Б., Сарьян В. К., Фокина А. А. Правовые аспекты внедрения интернета вещей // ИТ-Стандарт. 2015. № 4 (5). С. 9 – 16.

Комбинируя правовые, технологические и административные методы, можно обеспечить конфиденциальность и защиту личных данных в рамках международного, регионального и национального уровней.

Цифровое общество претерпело ряд изменений: если в период его становления большинство технологий были разработаны сугубо для организации взаимодействия без учета состояния информационной безопасности, то сегодня подавляющее большинство стран пришло к выводу, что информационная безопасность – это национальный приоритет.

В пособии представлена концепция, согласно которой информационная безопасность государства предполагает анализ информации как объекта правоотношений. Стандарт комплексной профилактики нарушений обязательных требований, утвержденный Протоколом заседания проектного комитета по основному направлению стратегического развития Российской Федерации «Реформа контрольной и надзорной деятельности» от 12 сентября 2017 года № 61, определил необходимость изменения контрольной и надзорной деятельности и глобальную взаимосвязь, взаимозависимость и взаимный симбиоз информационных, технических, управленческих и экономических отношений[1].

Сегодня законодателем отмечено, что информацию, которая создана в киберпространстве, можно трактовать как автономную имущественную ценность, но он никак не комментирует, что информация является объектом правоотношений.

Между тем Е. В. Богданов[2], О. В. Кириченко[1] и некоторые другие исследователи отмечают, что если бы информация была признана

---

[1] Стандарт комплексной профилактики нарушений обязательных требований (утв. Протоколом заседания проектного комитета по основному направлению стратегического развития Российской Федерации «Реформа контрольной и надзорной деятельности» от 12.09.2017 № 61(11)) (вместе с «Требованиями к структурированию и размещению сведений о мерах профилактики нарушений обязательных требований на официальном сайте контрольно-надзорного органа», «Порядком составления и ведения перечня типовых нарушений обязательных требований», «Порядком установления контрольно-надзорными органами обстоятельств для обоснованного объявления предостережений о недопустимости нарушений обязательных требований») / Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 14.09.2024).

[2] Богданов Е. В. Информация как объект гражданских правоотношений // Гражданское право. 2018. № 5. С. 29.

как объект гражданских правоотношений, это позволило бы качественно ее регулировать.

В то же время информационное право постулирует, что информацию необходимо рассматривать не только как имущественную, но и доказательственную ценность, если будет реализована валидная экспертиза информационных сигналов, отмеченных информационной системой и сохранившихся в ней. Например, юридическую значимость документов (на бумажном носителе) подтверждают реквизиты документа. У электронных документов юридическая значимость реализуется через электронную подпись. Однако киберсреда не располагает реквизитами, которые позволили бы законодательству определить доказательственное значение информации.

Законодатель, объясняя специфику правоприменения электронной подписи, в федеральном законе от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», поясняет ситуации, в которых допустимо ее применение: «при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий, в том числе в случаях, установленных другими федеральными законами» (ст. 1). Это говорит о том, что информационные отношения, возникшие в киберпространстве, не регламентируются, так же как не признается самостоятельное доказательственное значение информации в электронной форме.

Такая ситуация создаёт правовые барьеры внутри системы международного правового регулирования информационных soft отношений.

В 2018 году президент Российской Федерации В. В. Путин, обращаясь к Федеральному Собранию Российской Федерации, определил как приоритетные такие направления развития страны, как «разработка и применение национальных стандартов безопасного информационного взаимодействия»[2]. К 2025 году многие из них уже внедрены на практике в большинстве субъектов страны. Кроме того, от-

---

[1] Кириченко О. В. Информация как объект гражданских правоотношений // Современное право. 2014. № 9. С. 77 – 81.

[2] Послание Президента Федеральному Собранию Российской Федерации от 1 марта 2018 г. URL: http://www.kremlin.ru/events/president/news/56957. (дата обращения: 12.11.2024).

дельно была выделена разработка общей стратегии информационной безопасности компаний и процесса реагирования на кибератаки.

Сегодня дефиниция «информационная инфраструктура» констатируется в 50 нормативно-правовых актах Российской Федерации. Это сделано с целью обеспечения условий формирования отношений в киберпространстве.

Можно сделать вывод, что с точки зрения законодателя информационная структура – это континуум искусственной природы (симулякр), сказавшейся на классификации правоприменительного регулирования государственной, корпоративной или частной сфер взаимодействия. Таким образом, свойства этих видов детерминируют отличия в подходах и к образовательной системе, что проявляется в необходимости формирования не только правового сознания, правовой культуры, но и воспитания информационно-коммуникативной культуры у будущих педагогов.

Характеристика свойств инфраструктуры коррелирует в зависимости от критериев, выбранных исследователем. Например, А. Кларк к числу основных показателей информационной инфраструктуры отнес симбиоз, открытость, масштабность, дидактичность, взаимосвязь с практическим консорциумом. Для сравнения: О. Хансет трактует информационную инфраструктуру как развивающуюся, прозрачную, упорядоченную и неоднородную фундаментальную составляющую.

Анализируя концептуальные идеи зарубежных исследователей рассматриваемого феномена, можно констатировать, что теория информационной инфраструктуры, принятая еще в начале 1990-х годов как политическое кредо, как парадигма изыскания информационных векторов, до сих пор находится на стадии становления и развития.

Постепенная глобализация технологий привела к эволюции организации ресурса в его сетевой вид и в последующем включила ресурс в систему, т. е. информационную структуру в киберсреде.

Российские ученые рассматривали информационную инфраструктуру через призму отношений, опосредованных привлечением критической информационной инфраструктуры. Можно постулировать, что с точки зрения российского законодателя информационные инфраструктуры могут быть представлены в виде симбиоза информационно-телекоммуникационных парадигм, сетей связи, а также частных и государственных систем.

Стратегия развития информационного общества в России на 2017 – 2030 годы направлена на реализацию условий формирования цифровых метапредметных знаний. Опираясь на этот документ, можно сделать вывод, что национальные приоритеты Российской Федерации включают информационную и коммуникационную инфраструктуры, свободный доступ к телекоммуникационной системе, а также правовой статус электронных документов в системе документооборота.

Вопросы и задания для самостоятельной работы

1. Охарактеризуйте правовое понимание киберпространства.
2. Прокомментируйте основы для возникновения правовых дискуссий о регламентации образования в киберсреде.
3. В чем заключается сущность и идеологическая характеристика работы киберпространства в глобальной киберинформационной среде?
4. Как вы оцениваете технологические возможности ИИ, VR, AR с точки зрения правовой регламентации их деятельности?
5. Можно ли сегодня утверждать, что с точки зрения российского законодателя информационные инфраструктуры могут быть представлены в виде симбиоза информационно-телекоммуникационных парадигм, сетей связи, а также частных и государственных систем?

1.2. Специфика правового регулирования киберпространства

Развитие киберинформационных феноменов в сети Интернет, входящей в киберпространство, нуждается в их правовом осмыслении. Процессы глобализации инициировали создание международного киберпространства, включающего в себя информационные системы, разветвленные трансформационные структуры.

Современная инфраструктура информационного пространства в условиях глобализации создается вне единой национальной системы правового регулирования. В рамках одной цифровой платформы объединяются возможности применения и сочетания разных информационных приложений, вариабельного технологического программного обеспечения с целью повышения удобства интерфейса для пользователя (например, разработка мультилингвистических систем).

Специфика понимания информации и возможностей ее правового регулирования исходит из осознания целей ее появления в киберинформационном пространстве. Информация в цифровом обществе – главный ресурс, который можно соотнести с самыми высокими выгодами – как экономическими, социальными, так и политическими. Следовательно, главными категориями информации являются возможность ее мультипрочтения, полилингвизм и мультиформы. Для достижения такого качества информации в киберинформационном пространстве требуется интеграция, т. е. объединение различных информационных технологий, программных платформ, приложений киберпространства, которые позволяют информации выполнить трансграничное обращение.

Исследователь процессов влияния глобализации на международное право В. В. Богатырев отмечает, что «габитус, представляющий собой хранилище сложившихся способов нормативного регулирования поведения и элементов социального и культурного наследия, передающихся от поколения к поколению и сохраняющихся в социальных группах в течение длительного времени, играет как положительную, так и отрицательную роль»[1]. Исследователь подчеркивает, что положительная составляющая габитуса опирается на коллективное бессознательное, исходя из традиционно-нормативного понимания социокультурного кода. При разрушении этой системы префигуративностью (М. Мид) для социально-культурной и киберинформационной среды характерно возникновение кризисных индивидуальных, социальных форм реагирования, проявляющихся в новых формах противоправного поведения. Отрицательная составляющая габитуса исходит из сдерживания прогрессивного общественного развития, которое инициирует отставание правовой системы от постгуманистической социальной парадигмы на транснациональном уровне.

При анализе данных социологических исследований ценностей, проводимых Р. Инглхартом в 80 % стран всего мира, длящихся более 15 лет, было установлено, что интернет-технологии (ИТ), сеть Интернет, киберинформационное пространство привели к изменениям показателя индивидуальности. У респондентов, которые переехали в го-

[1] Богатырев В. В. Глобальные процессы в праве : монография / Федер. служба исполнения наказаний, Владим. юрид. ин-т Федер. службы исполнения наказаний. Владимир : ВЮИ ФСИН России, 2011. С. 117.

род из сельского поселения и таким образом попали в информационное глобальное пространство, выявилось изменение в нормативной регламентации экономических и социальных процессов. Это проявилось в том, что коллективизм, даже в его родовом понимании, трансформировался в коллективный индивидуализм, традиционная поленезависимость – в полезависимость. Появились новые международные лингвистические формы, понятные только активным пользователям киберинформационного пространства, например сложносоставные слова-неологизмы с первой частью «кибер-» (кибербезопасность, киберспорт, кибервойска и др.). Данные неологизмы употребляются в нормативно-правовых актах как российских, так и международных организаций и иных правовых документах[1]. В то же время сегодня отсутствует единообразие в соотношении национальных законов и международных договоров – каждое государство понимает сущность этих дефиниций по-своему, вне согласования с международным сообществом. Такой подход к пониманию неологизмов в сфере правовых норм приводит к необходимости выработки единообразной трактовки новых терминов и понятий, уточнения (герменевтического) семантических оснований, что важно для более точного перевода текста и его анализа.

Изменение в условиях цифровизации процессов социального взаимодействия инициировало возможность неограниченного доступа к информационным ресурсам. Благодаря развитию киберпространства стало возможным найти человека по фотографии, формировать новые государственные услуги, получать доступ к удаленной информации, помогающей, например, бороться с кибертерроризмом. В то же время существование подобных возможностей предполагает наличие серьёзных рисков (получение доступа к удаленной информации (невозможность удаления нежелательной переписки), ко всем электронным данным личности).

Киберпространство, являясь частью киберинформационного сегмента, представляет собой глобальную среду, включающую политическую, экономическую, социальную и духовную составляющие. Из анализа современной юридической литературы следует, что основными критериями киберпространства выступают:

[1] Международное право : учебник / отв. ред. С. А. Егоров. М. : Статут, 2015. С. 417.

– универсальность;
– транснациональность;
– атерриториальность;
– переходность;
– динамизм;
– глобализм;
– внегосударственность.

Таким образом, киберпространство включает в себя самый разнообразный спектр возможностей и потребностей индивида. Сегодня мы уже можем анализировать результаты трудовой, военной, культурной, юридической, экономической, научной, медийной, политической, индивидуальной деятельности человека, корпораций, искусственного интеллекта. В таком дискурсе можно говорить о новом статусе правоотношений, которые осуществляются посредством информационно-коммуникативных технологий (ИКТ), ИТ, искусственного интеллекта (ИИ). Поэтому особое значение получает интерпретация информации.

Информация – сложная дифференцированная поливалентная система, имеющая сложную, не всегда взаимообусловленную структуру. Информация может трактоваться исходя из ее конструктивного и деструктивного потенциалов. В. Н. Лопатин в своем исследовании анализирует правоприменительную практику дефиниции «вредная информация». Особенно важно понимание этой дефиниции в образовательной системе, например для возрастной маркировки изданий для несовершеннолетних[1].

В своей статье «Проблемы правовой защиты человека в информационной войне» В. Н. Лопатин обозначает, что вредная информация «не является конфиденциальной, но ее распространение и применение через сети коммуникаций наносит вред человеку, обществу и государству»[2]. Таким образом, при наличии вредной информации мы говорим о деструктивных информационных ресурсах, вредном софте, программном обеспечении, ИИ и т. д. Появление такой деструктивной информации может сформировать самые сложноструктурные

[1] Лопатин В. Н. Проблемы правовой защиты человека в информационной войне // Информационное право. 2014. № 6 (42). С. 18.

[2] Там же. С. 19.

риски в виде цифровой преступности, киберпреступности, кибертерроризма.

Информационная деятельность в киберсреде сегодня крайне разнообразна: так, вредная киберинформация появляется через механизмы фишинга, когда через ссылки в программное обеспечение пользователя доставляется вирус, который получает доступ к ограниченной конфиденциальной информации лиц, корпораций без их информирования и направлен на мошеннические действия, распространение вредной информации, вирусов в отношении любых лиц, желающих восстановить доступ к своим заблокированным гаджетам. Во многих государствах мира сегодня разрабатывается национальное законодательство, направленное на превенцию распространения вредной информации в киберсреде[1]. Очевидно, что в условиях усиления процесса сепарации и трансформации киберпространства в международную сеть решать вопрос правового регулирования, опираясь только на концепции национальной системы права, невозможно. Необходимо искать основу для выработки международного соглашения.

Вопрос о регулировании ИКТ ставился международным сообществом неоднократно:

1. В 2003 году в Женеве на Саммите по вопросам информационно-коммуникационных технологий и информационного общества Международный союз электросвязи (МСЭ) организовал Всемирную встречу на высшем уровне по вопросам информационного общества (ВВИО). В рамках работы саммита была обсуждена и принята Женевская декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии»[2]. ИКТ были проанализированы в контексте их неравномерного распространения между развитыми и развивающимися странами.

2. В 2005 году приняты Тунисское обязательство и Тунисская программа для информационного общества[3]. Проанализирован вопрос о корректности распределения сфер влияния в киберпростран-

[1] Жарова А. К. Международные правовые концепции борьбы с распространением вредной информации // Бизнес-информатика. 2010. № 4. С. 46 – 53.

[2] Журнал Организации Объединенных Наций. URL: http://www.un.org/russian/conferen/wsis/dec.pdf (дата обращения: 12.11.2021).

[3] Бачило И. Л. Природа информационных конфликтов. Конфликты в информационной сфере и их причины // Конфликты в информационной сфере: правовые аспекты / под ред. И. Л. Бачило. М. : Юрайт, 2025. С. 36.

стве, в частности монополия США. Констатировано, что ИКТ «являются эффективным инструментом содействия делу мира, безопасности и стабильности, усиления демократии, социальной сплоченности, надлежащего управления и верховенства права на национальном, региональном и международном уровнях»[1].

3. В 2006 году решение, вынесенное на заседании Форума по вопросам управления Интернетом (ФУИ), прошедшего в октябре – ноябре в Афинах, было поддержано ЕС касательно проблем интернационализации новых стратегий в интернет-управлении. Подобная дискуссия подняла проблему неравнозначного развития глобальной инфраструктуры. Такой дискурс очень важен для поиска новых путей сопровождения ресурсов развивающихся стран в киберпространстве на глобальном транснациональном уровне стандартов.

4. В 2010 году на всемирной встрече в Женеве поднят вопрос о создании государствами национальной стратегии ИКТ. В Послании Генерального секретаря ООН по случаю Всемирного дня телекоммуникации и информационного общества № 10-30082(R) от 17 мая 2010 года указывается, что в современном мире телекоммуникация представляет собой нечто большее, чем просто базовую услугу: она является средством, содействующим развитию, улучшению общества и спасению жизни людей[2].

Рост международной деятельности, связанной с применением информационно-коммуникативных технологий, инициирует создание профильных международных организаций, деятельность которых направлена на поиск и выработку предложений сотрудничества в самых разнообразных вопросах.

Значимая роль в разработке принципов и подходов в области международного правового регулирования сети Интернет, а такие киберпространства принадлежит ООН. Российская Федерация является

---

[1] Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» // Национальный правовой ресурс Республики Беларусь. URL: http://pravo.by/webnpa/text.asp?RN=P31000060 (дата обращения: 27.05.2024).

[2] Secretary-General's Message on World Telecommunication and Information Society Day – 17 May 2010 // UNIC.RU. URL: http://unhqappspub-01.un.org/lib/dhlrefweblog.nsf ; Официальный сайт информационного центра ООН в Москве. World governments embrace ICT e-strategies // UNIC.RU. URL: http://www.itu.int/net/pressoffice/press_releases/2010/19.aspx (дата обращения: 27.05.2024).

активным членом ООН. Совместными усилиями всеми странами-участницами ООН реализуются программы и поддерживается деятельность ее специализированных организаций.

В условиях роста глобализационного фактора и параллельно с ним глобализационных тенденций необходимо совместно осуществлять правовую регламентацию цифрового социально-экономического сектора. Российская Федерация демонстрирует высокий интерес и готовность к сотрудничеству в выработке вектора совместной правовой регламентации, определении правовых инструментов международного права для новых цифровых социально-экономических отношений в цифровой киберинформационной среде. Подобные инициативы в современных реалиях подвержены влиянию ряда факторов, которые затрудняют их конструктивную разработку и внедрение в практику. Так, например, санкции против России, введенные в 2014 году, привели к росту сегрегации, консолидации и привнесли правовые ограничения в область международного правового регулирования киберпространства.

В то же время ООН продолжает проводить дифференцированную поливекторную работу в области инновационных подходов к правовой регламентации современных ИКТ. DESA (United Nations Department of Economic and Social Affairs) – подразделение Департамента ООН по экономическим и социальным вопросам (ДЭСВ ООН) вносит большой вклад в исследовательскую работу, проводимую по различным политическим, экономическим, социальным, экологическим и цифровым направлениям. Нельзя не отметить, что ДЭСВ ООН является ведущим «авторским» департаментом Секретариата ООН. Публикации ДЭСВ ООН распространяются по всему миру, они состоят из аналитических отчетов, открытых исследований, межправительственных отчетов, необходимых для принятия наиболее глобальных политических решений в области, например, правового регулирования киберинформационного пространства.

Департамент занимается исследованиями и анализом киберпространства, киберугроз, кибертерроризма, поиском основы для цифрового международного правового сотрудничества через отдел государственных учреждений и цифрового правительства (Division for Public Institutions and Digital Government (DPIDG)), а также через лабораторию цифрового и мобильного управления (Lab for Digital and Mobile

Governance (DMG)). Значение превентивного вектора в отношении киберугроз, который реализует ООН, очень велико. Направление работы департамента сопряжено с актуальной для каждого пользователя сети Интернет проблемой информационной безопасности и обеспечивает поддержку Секретариата ООН для программы развития ООН в области государственного управления[1].

Постгуманистическая парадигма правового развития социума, ценностный релятивизм, новые симулякры киберсреды затронули и проблемы культурного наследия. Сегодня ЮНЕСКО постулирует важность работы по переходу к обществу знания. В качестве смыслообразующих принципов были выбраны:

– доступность образования;

– доступность информации;

– доступность свободы слова.

ЮНЕСКО реализует следующие программы в области развития ИКТ:

1. «Память мира».

2. «Информация для всех».

3. Международная программа развития коммуникаций.

4. Программа защиты цифрового наследия.

Содержательную часть Всемирной организации интеллектуальной собственности реализует постоянный комитет, отвечающий за информационные инновационные технологии, формирующий политическое кредо и предложения, направленные на совершенствование глобального информационного пространства.

Свои предложения Всемирная организация интеллектуальной собственности согласовывает с таким структурным подразделением ООН, как Генеральная Ассамблея, а также со специализированным консорциумом, в задачи которого входит организация дискуссионной панели для обсуждения информационных услуг виртуального мира, касающихся интеллектуальной собственности.

Анализ юридической литературы показывает, что подавляющее большинство государств разделяет концептуальные идеи, направленные на создание технологий, обеспечивающих безопасность и защиту

[1] Резолюции ГА 723 (VIII) от 23 октября 1953 года и ECOSOC резолюции 1199 (XLII) 24 мая 1967 года. URL: https://publicadministration.un.org/ru/About-Us/Who-We-Are (дата обращения: 27.05.2022).

как информационных, так и социальных систем от деструктивного посягательства, и на интеграцию информационных технологий, защищающих основополагающие звенья государств мира.

Характеризуя правовое регулирование киберсреды, отметим, что в этой сфере сосуществуют две амбивалентные концептуальные теории. Чем же они различаются? Содержательная характеристика первой концепции берет начало от момента зарождения Интернета, когда правовое регулирование интернет-среды даже не рассматривалось. Основоположник этой концепции Дж. Барлоу, заложивший ее характеристику в «Декларацию независимости киберпространства»[1], отстаивает идею плюрализма правового регулирования. Он опубликовал искомый документ как ответ на решение правительства США (1996) ввести цензуру в Интернете.

Сущность второй концепции состоит в аргументации постулата о том, что в интернет-пространстве правовое регулирование отношений жизненно необходимо, ибо в противном случае будет расти количество преступных посягательств на личность в виртуальном и реальном мире[2].

Своеобразие криминальных девиаций в виртуальном пространстве обусловлено тем, что личность преступника установить не просто. А. В. Минбалеев поясняет, что поскольку регламентировать отношения в киберсреде эффективно невозможно, остается один путь – применение норм права с целью регулирования отношений в виртуальном мире[3].

Сторонники и первой, и второй концепций, являясь достаточно известными специалистами в своей области, пытаются доказать состоятельность своих теорий. Исходя из принципа паритетности, мировое сообщество сознает, что, опираясь на принцип справедливости, каждый субъект имеет право на аргументацию своей теории. Выход из непростой ситуации видится в соблюдении принципа законности. Россия, как и многие страны Европы, заинтересована в разработке новых путей регулирования информационных отношений в киберсреде

[1] Barlow J. P. A Declaration of the Independence of Cyberspace. URL: http://www.eff.org/cyberspace-independence (дата обращения: 27.05.2022).

[2] Организация Объединенных Наций A/66/359. URL: https://www.rus.rusemb.org.uk/data/doc/internationalcoderus.pdf (дата обращения: 14.01.2022).

[3] Минбалеев А. В. Место и роль саморегулирования в развитии цифровых технологий // Образование и право. 2019. № 1. С. 253 – 256.

на национальном уровне. Подобные исследования обогащают национальное право для совершенствования государственной безопасности информационного пространства. Исходя из идеологической платформы государств, менталитета, национального права в целом, безусловно, направления, отвечающие за правовую регуляцию интернет-отношений, в разных странах имеют свою специфику. В то же время независимо от государственной политики и формы государственного устройства для всех государственных образований важны вопросы, направленные на упрочение безопасности, прежде всего, защита государственных интересов от деструктивного воздействия информации и глобальных рисков.

Вопросы и задания для самостоятельной работы

1. Что такое правосознание и какие структурные элементы оно включает?
2. Какова роль информационной грамотности в киберсреде?
3. Почему низкий уровень правосознания инициирует неправомерную поведенческую стратегию?
4. Как коррелируют между собой понятия «правосознание», «правовая культура», «правовое воспитание»?
5. Какими факторами обусловлено формирование правовой компетентности индивида?
6. Выделите объективные и субъективные факторы, приводящие к формированию низкой правовой и информационно-коммуникативной культуры в киберсреде.

Глава 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КИБЕРПРОСТРАНСТВЕ В УСЛОВИЯХ СОВРЕМЕННОГО ГЛОБАЛИЗАЦИОННОГО МИРА

2.1. Правовой аспект информационной безопасности киберпространства в России и за рубежом

Информационное пространство в мире переполнено дифференцированными смыслами и процессами. Регулярно в условиях глобализации появляются новые маршруты, технологии, софт, нуждающиеся в правовом определении. Рост глобализационных феноменов инициирует экономическая составляющая киберинформационного пространства.

В современных условиях необходимо переосмысление дефиниции «информационная безопасность» в правовом поле с учетом двух факторов:

1) глобализации;
2) киберсоциализационного релятивизма.

Анализируя юридическую, психологическую, социологическую литературу, касающуюся понятия «информационная безопасность в условиях глобализации», важно отметить, что оно характеризует методологию, раскрывающую безопасность как индивида, так и социума и государственных органов, касающуюся информационных паттернов экзогенного и эндогенного характера, чтобы сохранить качественную жизнь индивида, независимость страны, интеграцию различных социальных страт, а также поступательный экономический рост.

Детерминация киберинформационной средой ряда физических объектов и правовых отношений, взаимодействий, коммуникаций переводит их только виртуальное существование в симулякративное состояние. Силами одного государства создать механизм информационной безопасности невозможно.

Только в США существует около 600 нормативно-правовых актов, регламентирующих информационную безопасность (ИБ), например закон о неприкосновенности коммуникационных обменов, осуществляемых с помощью электронных средств. В то же время в 2006 году поступило 246 065 жалоб в FTC о краже личных данных и было зарегистрировано 8,9 миллиона случаев краж, мошенничества, преступлений в киберинформационной сети.

Таким образом, обороноспособность и суверенитет государств, с одной стороны, сталкиваются с интересами бизнес-сообщества транснациональных глобальных корпораций, с другой – с индивидуальным уровнем сформированности информационно-коммуникативной культуры в киберсреде.

Возникает серьезная проблема поиска способов упорядочивания киберинформационного пространства средствами международного права. В качестве примера можно привести ООН, выступающую главным инициатором поиска правового механизма регламентации отношений в киберинформационной среде. Рост использования гаджетов – самая статистически значимая данность XXI века. Для того чтобы понимать вектор изменения правовой нормы, дадим характеристику ситуациям, связанным с невозможностью технических компаний своевременно устранить уязвимость, благодаря которой можно легко получить доступ к персональным данным (TP-Link исправила прошивку TL_WR840N (EW-V5_211109) в 2021 году, но если пользователь своевременно не обновил устройство, то преступники могут беспрепятственно получить доступ к частным данным). Это позволяет десяткам тысяч технических устройств по всему миру MicroTick использоваться в ходе кибератак.

Специалисты компании Eclypsium констатируют, что больше всего уязвимых маршрутизаторов находятся в Китае, США, Бразилии, России, Индонезии и т. д.

В рамках национального права трудно препятствовать противозаконным операциям с цифровыми активами, так как существуют условно называемые «серые» зоны. Например, ни в одном законе нет четкого определения дефиниции «криптовалюта». При том что в ряде прецедентных решений цифровые валюты признаются имуществом, но нет единого алгоритма правоприменения.

Нельзя не отметить важность поддержки ООН, инициирующей совместно с ЮНЕСКО обеспечение и разработку проектов нормативной регламентации развития международного сотрудничества в сфере ИКТ.

МСЭ – важный правовой инструмент, координирующий приватные частные сектора для правительственных служб. В 1996 году ООН сформулировала принципы цифрового общества, исходя из политического и социального запросов, но не учла экономические цели

глобальных компаний. В 1998 году Российская Федерация внесла в повестку дня ООН обсуждение рисков ИБ и предложила первый в мире проект резолюции на заседании Первого комитета Генеральной Ассамблеи ООН.

Проект резолюции приняли без голосования (A/RES/53/70). Таким образом, Генеральная Ассамблея ООН и Генеральный секретарь ежегодно с 1998 года представляют информационный доклад об угрозах ИБ.

Например, в ноябре 2024 года было выявлено более 1 000 000 фейковых ресурсов о СВО. Рост включенности киберсреды в информационную войну инициирует необходимость усиления и структуризации механизмов правовой регламентации ИБ личности.

Новые схемы мошенников широко используются в социальной сети ВКонтакте, особенно в группах, в которых наблюдается большая активность, а количество участников достигает одного миллиона и более. Специально создаются панические настроения через публикации сомнительного контекста, например о Х-штамме нового вируса. Цель подобных «вбросов» – сбор данных о банковских картах через фишинг.

В 1999 году ООН обозначила, что достижения науки могут трансформировать проблемы гражданского и военного секторов государств. Была предложена инициатива создания Глобальной культуры кибербезопасности (Резолюция Генеральной Ассамблеи 64/211 «Создание глобальной культуры»).

С целью нивелирования деструктивных вызовов информационного пространства необходимо укреплять связи между государствами во всех областях и в первую очередь в сфере информационной и кибербезопасности как средств связи, так и Интернета, предназначение которых должно отвечать повышению материального благосостояния населения и экономическому росту государств, а также повышению коллективной международной безопасности.

Официальным документом ООН является проект государств – членов ШОС «Правила поведения в области обеспечения международной информационной безопасности (МИБ)», выступающий как результат заявленных постулатов.

Проект опирается на ряд принципов поведенческой стратегии государств: соблюдение положений Устава ООН и норм, оказываю-

щих регулирующее воздействие на международные отношения[1]; ограничение, вплоть до запрещения использования ИКТ и различных социальных сетей деструктивного и агрессивного характера, создающих угрозу международному миру и безопасности, популяризующих экстремистские направления; организация интегративного консорциума как инструмента борьбы с преступностью и терроризмом в виртуальной среде; создание безопасного пространства в области информационного поля и инфраструктур, а также инновационных информационных технологий[2].

Результаты работы 2010 года были представлены в резолюции A/RES/66/24, изданной в 2011 году Генеральной Ассамблеей ООН. В сентябре 2013 года была проведена 68-я сессия Генеральной Ассамблеи ООН, на которой правительственные эксперты проанализировали документ A/68/98491. Организация 68-й сессии Генеральной Ассамблеи во многом была аргументирована тем, что 48-е пленарное заседание, проведенное в 2012 году, обозначило потенциально опасные риски информационных технологий для реализации целей, имеющих негативное воздействие на государственные инфраструктуры и разрушающих безопасность в гражданских и военных областях[3].

В 2015 году правительственные эксперты рекомендовали государствам, входящим в ООН, ряд мер, укрепляющих безопасность и солидарность с Конвенцией о предотвращении киберпреступности[4].

Анализируя генеалогию событий, необходимо обратить внимание на то, что в принятой в 2016 году резолюции 71/28493 о развитии

---

[1] Минбалеев А. В. Правовое обеспечение кибербезопасности во Вьетнаме // Вестник УрФО. Безопасность в информационной сфере. 2019. № 1 (31). С. 64 – 68.

[2] Письмо постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 года на имя Генерального секретаря // Организация Объединенных Наций A/66/359. URL: https://www.rus.rusemb.org.uk/data/doc/internationalcoderus.pdf (дата обращения: 14.01.2024).

[3] Резолюция, принятая Генеральной Ассамблеей 21 декабря 2009 года [по докладу Второго комитета (A/64/422/Add.3)] 64/211. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур // Организация Объединенных Наций A/RES/64/211. URL: https://undocs.org/ru/A/RES/64/211 (дата обращения: 14.10.2024).

[4] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf (дата обращения: 04.01.2024).

в области информации и телекоммуникаций в контексте международной безопасности и совершенствования в информационной области в русле международной безопасности отмечалась роль диагностики и рекомендаций, адресованных государствам – членам ООН, которые необходимо было принять в формате международной безопасности и отразить в разрабатываемых концептуальных направлениях и потенциальных и реальных мерах. Меры, по мысли законодателя, включают глобальный и национальный уровни и ориентированы на оптимизацию положительных возможностей укрепления информационной (технологической и soft) безопасности на международном уровне.

Через два года, в 2017 и 2018 годах, были подведены итоги работы Департамента общественной информации, направленной на популяризацию работы ООН через оказание услуг в сфере стратегической коммуникации.

В контексте исследования основ нормативно-правового регулирования (информационной кибербезопасности), возникающих в социокультурной среде, важно выделить принципы формирования глобальной культуры кибербезопасности[1].

Первым принципом выступает информированность всех участников стратегической коммуникации. Второй принцип – ответственность, распространяющаяся на политические действия, затрагивающие безопасность информационных технологий и сетей.

Необходимость третьего принципа – реагирования – продиктована обменом информации об угрозах и принятием своевременных совместных мер по превенции компьютерных рисков и обеспечению успешного сотрудничества для их профилактики.

Принцип этики подразумевает соблюдение интересов всех участников современного консорциума. Принцип демократии предполагает реализацию соблюдения ценностей демократического социума, в том числе свободу слова и информации, тайны переговоров телефонного и телеграфного форматов, обеспечение надежной защиты сведений конфиденциального характера. Для выявления угроз и факторов их уязвимости применяется принцип оценки рисков. Его реализация предполагает, что существующая обширная база рисков учитывает эндогенные и экзогенные факторы, оказывающие влияние на ан-

[1] Resolutions 71st session. URL: http://www.un.org/en/ga/71/resolutions.shtml (дата обращения: 04.01.2023).

тропогенные условия, устойчивость технологий, методику, обеспечивающую стабильность функционирования информационной структуры. Поскольку основополагающим элементом реализации информационных маршрутов выступает безопасность, был введен принцип проектирования и внедрения методов, обеспечивающих информационную безопасность.

Безусловно, информационной безопасностью необходимо управлять. С этой целью был выявлен интегративный подход, оценивающий риски, охватывающие деятельность всех участников. Не менее важным принципом выступает переоценка, ориентированная на защиту правовых основ информационного блока и его надежности в глобальном мире.

Основополагающее условие самоактуализации международного симбиоза в сфере реализации защиты информации – дифференциация национальной специфики в методологии, направленная на обеспечение защиты информационного консорциума.

Обозначенные принципы зафиксированы в документах, раскрывающих аспекты международной защиты информации, лежащей в основе политического воззрения Российской Федерации. Пункт 11 Резолюции 71-й сессии ООН постулирует, что к значимым направлениям государственной политики России относятся условия, продвигающие российскую инициативу о принятии государствами – членами ООН конвенции, обеспечивающей международную информационную безопасность.

Следующим направлением, обозначенным в резолюции, выступает фасилитация в сфере выработки поведенческой стратегии, а также формировании континуума, обеспечивающего международную информационную безопасность и закрепляющего российскую инициативу в документах ООН в сфере информатизации и телекоммуникаций в рамках обеспечения международной безопасности.

Законодательство, разрабатываемое государствами – членами ООН, опирается на принципы международной информационной безопасности. В качестве примера можно привести Хорватию, в которой в конце 2014 года был принят закон о государственной информаци-

онной инфраструктуре, регулирующий информационные полномочия в сфере безопасности государственных органов[1].

Закон содержит технологические концепты, раскрывающие механизм функционирования информационных континуумов страны и конгломерат факторов, положенных в основу данного документа. Принятие подобного закон – важный шаг, помогающий интеграции Хорватии не только в европейские, но и в трансграничные виртуальные пространства.

Следовательно, организация государственных информационных служб – архисложная задача. Кроме Хорватии, такие законы приняли страны Юго-Восточной Азии, например Бруней-Даруссалам. Признав существование киберпреступности и кибертерроризма, государства постановили интегрировать усилия мирового континуума для организации надежного киберпространства[2].

С этой целью в структуре ООН было создано национальное агентство, цель которого – профилактика и нивелирование виртуальных провокаций. В рабочую группу ADMM-Plus вошли 18 государств, участвующих в защите киберпространства, подвергаемого атакам, вызванным ростом популярности мобильных устройств.

По мнению правительства Кубы, необходимо создать международно-нормативную базу в сфере ИКТ. Для продуктивной работы с государствами по защите их интересов в сфере информационных и телекоммуникационных систем следует разработать международный договор об интегративной помощи в области названной проблемы. В противном случае деструктивное использование информационных систем подрывает правовую и политическую основы государств, нарушает международное право и может привести к возникновению неблагоприятной ситуации и негативно влиять на целостность и безопасность государственной инфраструктуры. Правительство Кубы можно понять, поскольку политика США, проводимая против Острова свободы, включающая информационный контент, направлена на иска-

[1] Gršić B. State Secretary of the State Office for the Development of the Digital Society // Digital Public Administration Factsheets. Croatia, 2020. P. 30 – 48. URL: https://joinup.ec.europa.eu/sites/default/files/inline-iles/Digital_Public_Administration_Factsheets_Croatia_vFINAL.pdf (дата обращения: 05.12.2021).

[2] Seventy – second session Item 95 of the provisional agenda. Developments in the field of information and telecommunications in the context of international security Report of the Secretary – General. URL: http://undocs.org/A/72/315 (дата обращения: 05.11.2024).

жение основополагающих установок ООН в сфере международного права.

1947 год вошел в историю международного права как поворотный пункт в сфере укрепления информационной безопасности, поскольку был создан Международный союз электросвязи[1], участниками которого стали такие государства, как СССР, Бразилия, Китай, Пакистан, Иран. Основополагающая роль данной организации состояла в укреплении безопасности с опорой на ИКТ. Мировые лидеры, участвовавшие в его организации, поручили принять меры, направленные на предотвращение внешней агрессии и дестабилизации.

В 2015 году была создана исследовательская комиссия ITU-T «Интернет вещей» (IoT) и «Умные города и сообщества» (SC&C). Комиссия выработала рекомендации для инновационных и информационных технологий, направленных на инновационные цифровые трансформации городской среды (например, возможность моделирования погодных условий, дифференцированных форм адаптации человека к урбанистической среде и др.). Таким образом, работа ITU-T направлена в сторону увеличения доли информационной инфраструктуры как в экономической, политической, так и социально-урбанистической сферах.

К 2019 году членами Всемирной ассамблеи по стандартизации электросвязи (ВАСЭ) являлись 193 государства, 700 институтов, 500 из которых представляли Россию, страны СНГ, Европы, Северной и Южной Америки, Юго-Восточной Азии. Резолюции этой организации послужили базисом для инициирования основополагающих стратегических направлений в сфере стандартизации международной электросвязи, позволивших национальным российским сетям стать структурным компонентом всемирной инфокоммуникационной инфраструктуры.

К 2020 году Международный союз электросвязи сориентировался на реализацию потребностей развивающихся стран и стал уделять большое внимание вопросам, поддерживающим информационное просвещение в области дифференцированных цифровых технологий,

[1] Developments in the field of information and telecommunications in the context of international security Report of the Secretary – General. URL: http://undocs.org/A/72/315 (дата обращения: 05.11.2024).

в частности в профилактике и нивелировании последствий ЧС при изменениях климата.

Таким образом, сегодня необходимо выбрать международный правовой подход к пониманию дефиниции «информационная безопасность», проанализировать ее детерминацию глобализационными, цифровыми феноменами. Правовые инициативы МСЭ-Т и России исходят из целеполагания и потребности инициации развития всех социальных сфер в их макроформате глобального мира. Несомненно, изменение правовой среды может влиять на такие глобальные проблемы, как изменение климата, терроризм, нивелирование культурных ценностей, нищета. Следовательно, правовая регламентация и упорядоченность цифрового сегмента политической, социальной, духовной и экономической сфер будут способствовать росту безопасных условий правоотношений и взаимодействий.

Программа Минкомсвязи России «Цифровая экономика Российской Федерации» включает в себя анализ параметров информационной, технологической и soft безопасности[1]. В то же время ЕС принимает перечень документов, направленных на снижение финансовых рисков из-за правовых инцидентов в цифровом сегменте экономики[2].

В программе отражены алгоритмы международного права в области нормотворчества, направленные на устранение криминальной составляющей виртуального пространства. В частности, апологеты международного консорциума считают, что в виртуальном мире не должно быть популяризации деструктивного содержания и любых противозаконных текстов.

---

[1] Приказ Минкомсвязи России от 11 июня 2019 г. № 278 «Об определении официальных сайтов в информационно-телекоммуникационной сети «Интернет» оператора единого реестра российских программ для электронных вычислительных машин и баз данных и оператора единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru. (дата обращения: 14.09.2021).

[2] Рекомендация № R (87), направленная на обеспечение безопасности персональных данных; Рекомендация № R (95) о защите персональных данных в сфере телекоммуникационных услуг (1995) ; Рекомендация № R (95) по уголовному процессу, связанному с информационными технологиями ; Конвенция о преступлениях в сфере компьютерной информации (30 стран-участниц) (1996 – 2001 гг.). Россия не является ее участницей ; интегративный документ между ЕС и НАТО ; директива по безопасности сети и информационных систем Европейского парламента и Совета Европы (Network and information systems across the Union – NIS504 (далее – Директива NIS)).

Глобальные транснациональные организации должны действовать как конструктивные сообщества, действия которых направлены на поиск и ликвидацию криминальных девиаций в киберпространстве.

Одно из важных направлений современной действительности – соблюдение авторских и смежных прав, поэтому деятельность международных организаций должна быть направлена на предупреждение искажения информации в виртуальном пространстве.

Международный консорциум должен выработать рекомендации, реализующие сохранение информации личного характера, и устранять любые девиации, нарушающие личное пространство индивида.

Программа – своеобразное обращение к государствам ЕС, призывающее усовершенствовать национальное право, привнеся в него наказания уголовного характера за действия против личности.

Директива NIS предполагает рассмотрение функционала стран, входящих в ЕС, с целью совершенствования правовой регламентации, позволяющей нивелировать деформацию информационного содержания через трансформацию форм международного взаимодействия, выявление и открытость данных для международного сотрудничества[1].

Положения Директивы NIS также не должны применяться к поставщикам услуг доверия, отношения с которыми регулирует регламент (ЕС) № 910/2014 Европейского парламента и Совета[2]. В 2003 году Комитет министров Совета Европы отменил Конвенцию о преступности в сфере компьютерной информации, Рекомендацию Rec (2001) о саморегулировании виртуального содержания, а также Директиву 2000/31/ЕС Европарламента и Совета ЕС от 8 июня 2000 года о правовых аспектах услуг в сетевом обществе, признав их противоречащими демократическим принципам[3].

---

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG (дата обращения: 04.01.2021).

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC // OJ. L.257. 28.8.2014. P. 73.

[3] E-Commerce Directive. URL: https://ec.europa.eu/digital-single-market/en/e-commerce-directive (дата обращения: 24.12.2019).

Комитет министров разработал и постановил применять принципиально новые подходы в киберкоммуникациях в Совете Европы. Было сформулировано семь принципов в области обмена информацией в Интернете: отсутствие ограничения в области объема, обмена и доступа к информации; альтернативная возможность признания ее компетентными национальными органами незаконной; государственное и саморегулирование или совместное регулирование в отношении информации, распространяемой через Интернет. Четвёртый принцип подразумевает, что государства – члены Совета Европы должны обеспечивать и поощрять доступ всех лиц к информации, содержащейся в киберсреде, и информационным услугам на недискриминационной основе по приемлемым ценам. Кроме того, активное участие населения, например, в разработке индивидуальных веб-сайтов не подлежит лицензированию или оно не обязано выполнять аналогичные требования. В пятом и шестом принципах поднимается вопрос о создании разрешительных схем и стимулировании развития таких масштабных киберпроектов, как «Интернет вещей», «Умный город», самых дифференцированных предложений в сфере цифровой экономики и коммуникации. Выявлены большая неопределённость, характеризующая действия провайдеров, главным параметром которой выступает полный доступ к национальной информации, и неприемлемость инициации осуществления провайдером ее мониторинга в киберсреде, например, для выявления противоправной деятельности[1].

Седьмой принцип позволяет не раскрывать свою личность пользователям Интернета.

Российская Федерация не присоединилась к данной конвенции, так как принципы международного сотрудничества, анонсированные ранее, противоречат принципам регулирования общественных отношений в нашей стране.

В то же время Россия, обеспокоенная угрозами киберпреступности, стала инициатором подготовки проекта, направленного на противодействие этой угрозе. Международное сообщество, «разделяющее» опасения России, тем не менее не поддержало эту инициативу.

[1] European Convention for the Protection of Human Rights and Fundamental Freedoms. URL: https://en.wikisource.org/wiki/European_Convention_for_the_Protection_of_Human_Rights_and_Fundamental_Freedoms (дата обращения: 04.01.2020).

А. Н. Савенков подчеркивает, что сегодня необходим документ, исключающий амбивалентные тезисы о нарушениях в сфере виртуальной информации, опирающийся на позитивный опыт предыдущих конвенций, уважающий основополагающие принципы норм международного права и интересы всего международного сообщества. Красной нитью в документе должен проходить унифицированный подход к решению исследуемой проблемы.

Предложенная в 2012 году Россией конвенция отличалась в своем содержательном аспекте от документа, принятого Советом Европы, так как рассматривала конкретные внешнеполитические действия государств в информационной среде, в то время как конвенция Совета Европы была ориентирована на ликвидацию киберпреступлений, в частности кибермошенничества, распространения детской порнографии (например секстинга), угрожающих как физическим, так и юридическим лицам.

Если разработчики документа Совета Европы включили дефиницию «информационная война» и механизм информационного психологического воздействия на социум и государство, то авторы отечественной конвенции направили ее содержание на закрепление правового регулирования государств национальных сегментов Интернета. Национальные правовые доктрины российской конвенции вызвали критику у западноевропейских и американских коллег из-за разных трактовок структурной составляющей дефиниций «информационная безопасность» и «цензура». В одной из критических форм анализа документа в США указана недопустимость легитимизации цензуры в контексте нарушения политических и гражданских прав человека[1]. Автор не разделяет данное положение, поскольку конвенция не отменяет действие Международного пакта о гражданских и политических правах, действующего независимо от конвенции.

Правовое регулирование информационной безопасности больших систем информационных данных нуждается в регламентации, особенно в той части, которая связана с определением, пониманием, способами выявления вредной информации. В международной системе правового регулирования национальный плюрализм в трактовке

[1] Савенков А. Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 5.

дефиниций «безопасность», «информация», «вредная информация», «Интернет вещей» создает необходимость выработки единых категорий в понимании содержания и действия цифровых феноменов в социальной, политической, экономической и духовной сферах применения.

В ЕС безопасные информационные системы регулируются ст. 13а Рамочной директивы (2009/140 / ЕС) и Европейским агентством сетевой и информационной безопасности (ENISA)[1].

ENISA представляет собой организацию ЕС, отвечающую за систематизацию киберучений и выявление основополагающих требований к безопасности информационного пространства.

Рекомендация № R (99) 14 об универсальных услугах в отношении новых средств связи и информационных служб[2] определила меры, направленные на обеспечение безопасности соединения через установленные точки открытого доступа.

С целью реализации электронных транзакций в условиях внутреннего рынка разработан Регламент (ЕС) № 910/2014516. Созданию общей системы сертификации информационных структур в 2018 году способствовала инициатива Европейского Совета, предложившего Комиссии ООН разработать пакет предложений, обеспечивающих информационную безопасность[3].

Инициирование принятия закона об информационной безопасности, предусматривающего варианты политической стратегии с вовлечением сертификации ENISA и информационной безопасности (ИКТ), принадлежит Европейской комиссии, рассмотревшей этот документ в 2018 году. Его фундаментом стала европейская платформа

---

[1] DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0140 (дата обращения: 04.01.2021).

[2] Recommendation № R (99) 14 of the Committee of Ministers to member states on universal community service concerning new communication and information services. URL: https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-no-r-99-14-of-the-committee-of-ministers-to-member-states-on-universal-community-service-concerning-new-communication-and-information-s?inheritRedirect=false (дата обращения: 05.01.2024).

[3] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the «EU Cybersecurity Agency», and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification («Cybersecurity Act») – General approach. URL: https://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf (дата обращения: 04.11.2024).

сертификации в сфере виртуальной безопасности продуктов и услуг в области ИКТ, детерминирующая сертификационный анализ, позволяющий им выполнять функции законотворческих актов. Нельзя не отметить, что к функциям ЕС относятся создание единой информационной инфраструктуры, обеспечивающей симбиоз въезда/выезда (EES); организация (VIS) визовой информационной системы, а также Шенгенской и Европейской систем сбора информации о преступлениях против личности и общества для населения. В современных условиях создание информационной инфраструктуры должно происходить максимально глобально, вне глокализационных барьеров для получения дифференцированных данных.

С 2016 года информационная инфраструктура единого пространства выстраивается поливариативно, ведется поиск основ для его правового регулирования, исследуются существующие преимущества ИТ и информационных систем, создаются инновационные блоки программ для адаптации систем к новым рискам и повышения их интегративной способности относительно друг друга. Примеры подобных составных частей информационной структуры – системы въезда/выезда (EES), Европейская система информации о путешествиях (ETIAS), Шенгенская информационная система (SIS), Европейская информационная система уголовных сообщений для граждан третьих стран (ECRIS-TCN), Европейский поисковый портал (ESP), общее резидентное хранилище (CIR), Детектор множественного идентификатора (MID). Например, Германия солидарна с методами применения международного законодательства, регулирующего национальное использование ИКТ, включая нормы технического регулирования, правила и принципы ответственной поведенческой стратегии государств, ориентированных на формирование открытой, безопасной, непоколебимой, конструктивной ИКТ. Правительственные эксперты, работающие в сфере развития, создания и использования информационного контента, помогают осуществлять меры, укрепляющие доверие и направленные на поддержание безопасности в случае государственного использования ИКТ.

В 2015 году был принят закон «О технике безопасности» (пересмотрен в 2016 году), направленный на инициирование создания института международной кибербезопасности для систематизации усилий, выступающих национальными мерами регулирования. Можно

утверждать, что усилия Германии по укреплению безопасности ИКТ – составная часть международной безопасности. Кроме Германии, Греция ратифицировала Конвенцию о преступлениях в информационной сфере, а также дополнительный протокол к этому документу, рассматривающий противоправные действия, обусловленные тиражированием расизма и ксенофобии в компьютерных системах.

Страны ЕС совершенствуют процедуры ответа на ситуации, возникающие в информационном пространстве. В частности, создаются группы, разворачивающие свою деятельность в кратчайшие сроки с целью устранения последствий атак в виртуальном мире, в том числе в военных или социальных сетях. Цель политических документов – упорядочивание нормотворческих процедур, направленных на восстановление компьютерных сбоев, полученных вследствие кибератак.

Согласованная работа информационных континуумов стран – членов Евросоюза дает возможность унифицировать требования, направленные на эффективное использование данных Европола, Интерпола через доступ соответствующих структур.

Вопросы и задания для самостоятельной работы

1. Охарактеризуйте правовые подходы отечественных ученых, лежащие в основе формирования информационной безопасности киберпространства в России и за рубежом.

2. Чем обусловлен выбор принципов, лежащих в основе модели формирования правового сознания студентов – будущих педагогов (рис. 1)?

3. Аргументируйте выбор критериев (см. рис. 1), лежащих в основе формирования информационной безопасности киберпространства в России и за рубежом средствами информационно-коммуникативной культуры.

4. Охарактеризуйте информационные структуры киберсреды.

5. Коррелируют ли между собой уровни сознания и правовой культуры?

6. Проанализируйте возможности воспитания информационно-коммуникативной среды по приведенной модели (рис. 1).

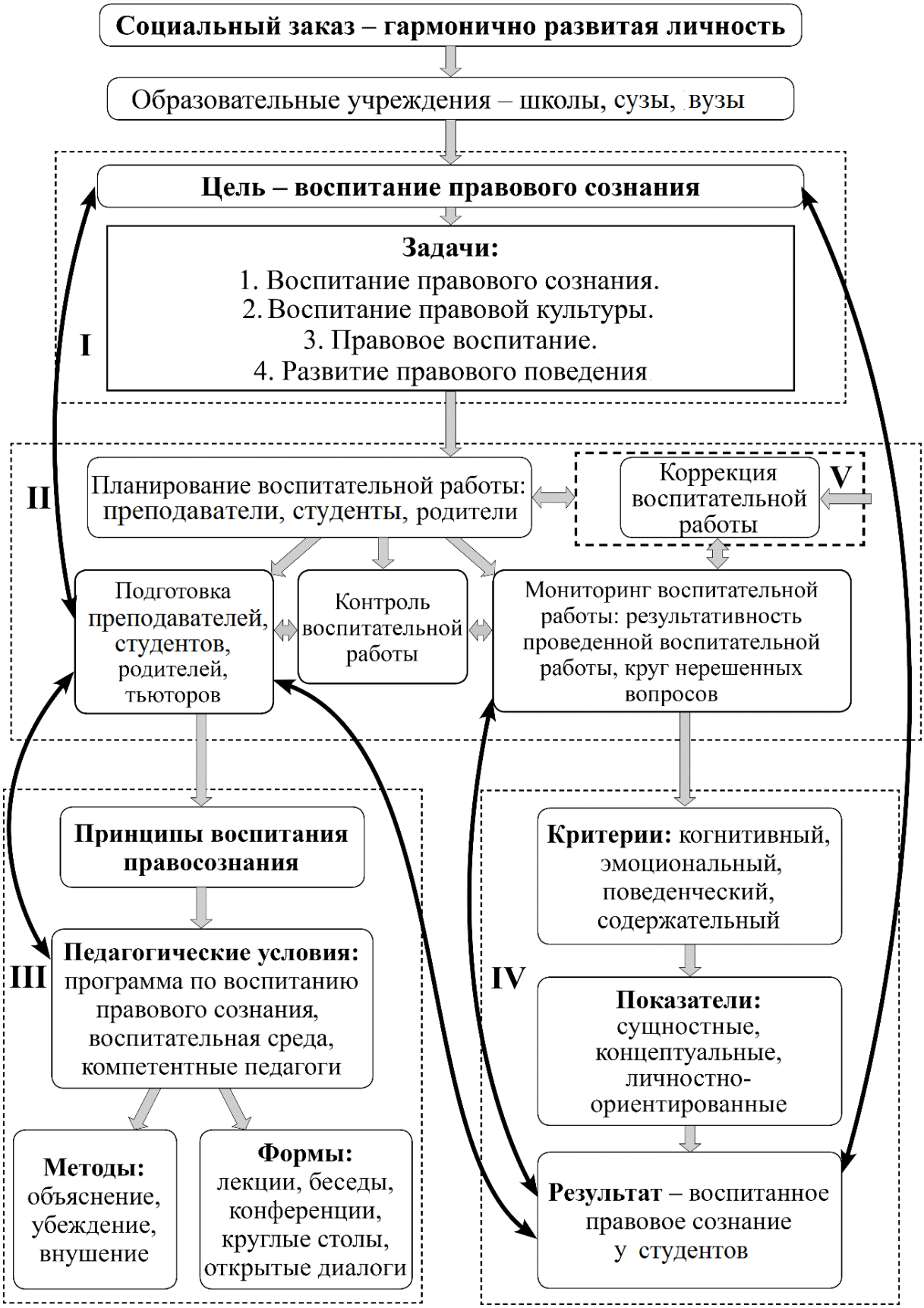

Рис. 1. Модель воспитания правового сознания студентов – будущих педагогов

2.2. Правовое обеспечение противодействия деструктивной информации в сети Интернет

В России существует большое количество рисков, связанных с невозможностью ограничения воздействия на деструктивную информацию, имеющую социальное и личное значение для человека.

В современных реалиях есть большое количество приложений, связанных с определением телефонных номеров, которые не регламентируются никакими правовыми актами, в том числе осуществляется выставление рейтингов пользователям, которые могут принести репутационные риски. Например, столь популярное приложение GetContact, с одной стороны, показывает выборочно факты записи контакта в личных телефонных книгах, с другой – позволяет через Интернет добавить к одному номеру большое количество наименований, которые могут содержать как реальную, так и вымышленную вредоносную информацию об абоненте. О выборочности данных можно судить по неполному соответствию вносимых баз данных из телефонных книг абонентов в общее публичное информационное пространство Интернет. Любой пользователь GetContact может присвоить любой тег любому телефонному номеру, не опасаясь административной ответственности. Программа показывает в большом количестве оскорбительные теги, чужие имена и не соответствующую реальному владельцу телефонного номера информацию. При этом программа GetContact установлена в 146 странах.

Правовая регламентация определения рейтинга номеров, качества абонентов нуждается в серьезном правовом осмыслении, поскольку может причинить реальный вред из-за преступных посягательств на предоставление конфиденциальной информации об абоненте для широкого круга лиц с неверной интерпретацией. Например, номер обычного абонента можно отметить как спам, таким образом снизив его возможности вести профессиональную и социальную активность, при этом он даже не будет знать об этом.

Исследователи Дж. Х. Сарах и С. Т. Миддельбрук постулируют, что на протяжении долгого исторического периода развития человеческой цивилизации развивалось право, изменялись денежные системы, какие-то исчезали, на смену им приходили новые, качественно

иные формы[1]. Во многих странах эквивалентом стоимости определенного товара выступала не только признанная валюта. В разные исторические периоды использовались и натуральный обмен, и эквивалентная по ценности с валютой мера стоимости товара, например в Древней Руси такой единицей выступал беличий мех.

Цифровизация ряда экономических процедур позволила ввести альтернативные денежные единицы – криптовалюту. Такая денежная единица, не признанная во многих государствах, все равно используется при осуществлении экономических видов деятельности с движимыми и недвижимыми активами в киберинформационной сети[2].

В 2018 году государственный сектор включает в свою информационную систему блокчейн-технологии. В 2021 году технологии блокчейн максимально используют в экономических секторах взаимодействий[3]. Аналитическое агентство TAdviser приводит статистические данные общего объёма рынка блокчейн-проектов, который за 2018 – 2019 годы составил около 17 млн долл.[4].

В Беларуси декрет от 21 декабря 2017 года № 8 «О развитии цифровой экономики»[5] легализовал условия работы для блоков транзакций (блокчейн), производство и операции с криптовалютой (майнинг). Юридическое лицо, физические лица имеют право владеть, распоряжаться токенами, которые можно не декларировать, но в то же время они регламентируются по трудовому, гражданско-правовому договору. Таким образом, блокчейн создал условия для появления информации, которая служит средством платежа[6].

---

[1] Sarah J. X., Middlebrook S. T. Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries. № 32. 2015. URL: http://digitalcommons.law.yale.edu/yjreg/vol32/iss2/8 (дата обращения: 01.11.2019).

[2] Кожевникова Ю. Как блокчейн и распределенные реестры преобразят рынок недвижимости. URL: https://realty.rbc.ru/news (дата обращения: 01.02.2020).

[3] Клочкова Ю. А. Трансформация понятия «федерализм» в контексте европейской интеграции // Международное публичное и частное право. 2009. № 3. URL: http://lawinfo.ru/catalog/contents-2009/mezhdunarodnoe,-publichnoe-i-chastnoe-pravo/3/ (дата обращения: 01.02.2020).

[4] Аналитическое агентство TAdviser. URL: http://www.tadviser.ru/index.php (дата обращения: 01.02.2021).

[5] Национальный правовой ресурс Республики Беларусь. URL: http://pravo.by/webnpa/text.asp?RN=P31000060 (дата обращения: 27.05.2021).

[6] Грибанов Д. В. Деятельность субъектов общественного контроля и развитие систем распределенных вычислений и распределенного хранения данных // Право и управление. XXI век. 2018. № 1 (46). С. 14 – 22.

Сегодня отмечается необходимость анализа криптовалюты, которая имеет неопределенный правовой статус, не подпадая под ясную регламентацию существующих законов. В России есть прецеденты, когда криптовалюту (биткойны) – пиринговую платежную систему – используют для оплаты товаров.

В. В. Недорезков[1] обращает внимание на то, что в Российской Федерации до 2011 года не было разработано специального нормативно-правового акта, документа, регламентирующего специфические особенности обращения и выпуска электронных денежных средств. В 2011 году после принятия закона «О национальной платежной системе» появились основания для предметного правового дискурса[2] о реальных возможностях определения правового статуса биткойна.

В соответствии с ч. 1 ст. 75 Конституции Российской Федерации денежной единицей страны является рубль. Денежную эмиссию осуществляет исключительно Центральный банк РФ. Таким образом, криптовалюта, электронные денежные средства не могут быть выпущены вне контроля государства и Центрального банка. До тех пор пока не будет дано четкого понятия денежного суррогата в теории права, говорить о правовой легализации криптовалюты трудно.

В соответствии со ст. 27 федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации» введение на территории России других денежных единиц и выпуск денежных суррогатов запрещены.

В соответствии с п. 18 ст. 3 закона № 161-ФЗ «О национальной платежной системе» под электронными денежными средствами понимаются «денежные средства, которые предварительно предоставлены одним лицом другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств

[1] Недорезков В. В. Криптовалюты на базе технологии блокчейна: проблемы правового регулирования // Банковское право. 2017. № 4. С. 45 – 49.

[2] Ciaian P., Rajcaniova M., d'Artis K. Virtual relationships: Short – and long – run evidence from BitCoin and altcoin markets // Finansic Markets Institute Money. 2018. № 52. P. 173 – 195.

платежа». Законодатель на современном этапе развития права исключает возможность отнести криптовалюту, в частности биткойн, эфириум, к денежным единицам.

Дефиниция «электронные деньги» в соответствии с п. 1.4 Положения о правилах осуществления перевода денежных средств не подобна категории киберсреды «кибервалюта». И биткойн, и электронные деньги на первый взгляд имеют предоплаченный характер, но на этом процессуальная схожесть заканчивается. Важным правовым аргументом выступает констатация отсутствия потребности в наличии счета в финансовых организациях для перечисления биткойнов. Блокчейн-технология позволяет обходиться без счета, таким образом минуя многие обязательные налоги[1].

Биткойн не является и средством наличного платежа на территории иностранного государства или группы иностранных государств (п. 1 и 2 ч. 1 ст. 1 федерального закона от 10 декабря 2003 года № 173-ФЗ «О валютном регулировании и валютном контроле»[2]).

В то же время в руководстве Финансового департамента США (FinCEN) отмечается, что федеральными правилами криптовалюта отнесена к «реальной валюте», такой же как монеты и банкноты США или иностранного государства[3].

В ст. 128 ГК РФ к объектам гражданских прав отнесены: вещи, включая наличные деньги и документарные ценные бумаги, иное имущество, в том числе бездокументарные ценные бумаги, безналичные денежные средства, результаты работ и оказание услуг; имущественные права; охраняемые результаты интеллектуальной деятельности и приравненные к ним нематериальные блага и средства индивидуализации. Исходя из этого, криптовалюта может выступать объектом гражданско-правовых отношений.

---

[1] Положение о правилах осуществления перевода денежных средств : утв. Банком России 19 июня 2012 г. № 383-П // Вестник Банка России. 2012. № 34. С. 3 – 44.

[2] О валютном регулировании и валютном контроле : федер. закон от 10 дек. 2003 г. № 173-ФЗ // Собр. законодательства Рос. Федерации. 2003. № 50. Ст. 4859. URL: https://www.szrf.ru/(дата обращения: 22.01.2019).

[3] An official website of the United States Government. URL: https://fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block (дата обращения: 22.01.2019).

Криптовалюты (биткойн и эфириум) не входят в классификацию, предъявляемую к денежным единицам, так как не являются материальными объектами и не имеют общих родовых характеристик.

Биткойн не имеет юридического определения. В то же время он активно используется в международных экономических операциях.

Следовательно, виртуальные деньги не являются собственностью, так как собственность как юридическая категория предполагает право владения, распоряжения, пользования материальными объектами.

Информация – нематериальный объект. Исходя из ее нематериальности, законодатель юридически трактует это понятие, опираясь на дефиницию «обладание» (например, интеллектуальными правами можно обладать).

Минфин РФ неоднократно предлагал классифицировать криптовалюты как актив. Такая классификация позволит потенциальным инвесторам, компаниям покупать, продавать, обменивать ее, а также регулировать дифференцированные правовые риски с использованием криптовалюты.

Сегодня в России держатели криптовалюты имеют активы свыше 3 трлн руб. Таким образом, не регламентируемая законом единица, имеющая финансовый эквивалент, активно участвует в финансовом пространстве вне правового определения. Вопросы, касающиеся налогообложения, остаются открытыми[1].

Аналогичное мнение высказывают зарубежные исследователи Дж. Х. Сарах и С. Т. Миддлбрук[2]. Спекулятивный характер криптовалюты, реализация на виртуальных рынках особенно выросли в период пандемии и сопряжены с высокими рисками[3]. В серой зоне Darknet такая ситуация провоцирует неправовые гражданские инициативы. Это происходит из-за крайне высокого курса биткойна по отношению к любой национальной валюте на неофициальных биржах. В законе «О противодействии легализации (отмыванию) доходов, полученных

[1] Vandezande N. Virtual currencies under EU anti – money laundering law // Computer law & Security review. 2017. № 33. P. 341 – 353.

[2] Sarah J. X., Middlebrook S. T. Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries. 2015. № 32. URL: http://digitalcommons.law.yale.edu/yjreg/vol32/iss2/8 (дата обращения: 01.11.2019).

[3] Wanga H., Debiao He., Ji Y. Designated – verifier proof of assets for bitcoin exchange using elliptic curve cryptography // Future Generation Computer Systems. 2017. P. 207.

преступным путем, и финансированию терроризма» прописана ответственность юридических лиц при выявлении юридических фактов, подпадающих под его директивы. Неоднократно Минфин РФ предоставлял информацию о рисках, сопряженных с применением биткойна в незаконных финансовых операциях. Например, непризнанная денежная единица часто фиксируется в финансировании террористических организаций.

В то же время курс криптовалюты по отношению к мировым валютам растет. Сегодня за биткойн можно получить более 83 тыс. долл., или более 7 млн руб. (март 2025 года). Помимо биткойна, лидером на интернет-рынках является криптовалюта эфириум. В пособии приведены суммы, анонсируемые на интернет-ресурсах, чтобы показать высокий уровень спроса на криптовалюты. Исследователи П. Киаиан[1] и Х. Вандезанд[2] считают, что спекулятивный характер криптовалюты не сможет вывести биткойн на уровень конкуренции с существующими валютами.

Все большее количество ученых предлагают рассматривать криптовалюты как платежную систему, применяемую с помощью блокчейн-технологии. Транзакции с помощью криптовалюты возможны в ряде иностранных государств[3], но не в России.

Сегодня под платежной системой в Российской Федерации понимается «совокупность организаций, взаимодействующих по правилам платежной системы в целях осуществления перевода денежных средств, включающей оператора платежной системы, операторов услуг платежной инфраструктуры и участников платежной системы, из которых как минимум три организации являются операторами по переводу денежных средств»[4]. Следовательно, юридические лица, включающие в свою деятельность оборот криптовалюты, не могут обеспечить ни ее безопасность, ни ее законность.

В ст. 12 федерального закона «О национальной платежной системе» законодатель четко регламентирует, что только операторы электронных денег могут осуществлять с ними операции (платежи,

[1] Ciaian P., Rajcaniova M., d'Artis K. Op. cit. P. 173 – 195.

[2] Vandezande N. Op. cit. P. 341 – 353.

[3] Wanga H., Debiao He., Ji Y. Op. cit. P. 207.

[4] П. 20 ст. 3 Закона «О национальной платежной системе». Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.11.2019).

переводы и т. д.). В киберпространстве в «Интернете вещей» ситуация коренным образом меняется. Курс биткойна и эфириума растет, правовые регламентации по ним во многих государствах отсутствуют. В то же время в 2020 году в Сальвадоре президент Найиб Букеле принял биткойн как официальную валюту страны. Прецедент пояснил директор проекта Bitcoin Beach, занимающегося продвижением криптовалюты в Сальвадоре, Майк Петерсон. В Сальвадоре многие граждане не имеют банковских счетов, платежных приложений. Введение биткойна как официальной валюты предоставляет сальвадорцам возможность почти без комиссии осуществлять денежные переводы, проводить финансовые операции онлайн в «Интернете вещей» без ограничений. Страна, по подсчетам финансистов, экономит более 400 млрд долл. на комиссиях. Для совершения оплат в биткойнах разработано приложение Chivo – официальный криптовалютный кошелек[1].

В Российской Федерации запрещены введение иных денежных единиц и выдача денежных суррогатов (ст. 27 закона «О Центральном банке Российской Федерации (Банке России)»). И биткойн не может быть отнесен ни к электронным деньгам, ни к платёжной системе. Но прецедентная ситуация с частичной легализацией криптовалют создает условия для возникновения «серой зоны» в киберэкономическом пространстве.

В ч. 1 ст. 75 Конституции Российской Федерации запрещены ввод и эмиссия других денег в государстве. Таким образом, криптовалюта не может быть легализована.

В ст. 15.24.1 КоАП РФ за незаконную выдачу либо обращение ценных бумаг или удостоверяющих денежные и иные обязательства и не являющихся ценными бумагами в соответствии с законодательством документов предусмотрено наложение административного штрафа на должностные лица в размере от 30 до 50 тыс. руб. или дисквалификация на срок от одного до двух лет; на юридических лиц – от 700 тыс. до 1 млн руб.

Подобная противоречивая ситуация неопределенной правовой регуляции криптовалюты должна быть пересмотрена законодателем в соответствии с современной ситуацией, так как стоимость биткойна

[1] Биткоин стал официальной валютой в Сальвадоре. Финансисты сомневаются, что это хорошо закончится. URL: https://www.bbc.com/russian/news-58466367 (дата обращения: 01.02.2020).

выше 3 000 000 руб. и штрафы, при отсутствии налогообложения, не являются сдерживающим фактором для держателей криптовалюты, что создает основу для мошенничества и спекуляций в «серой зоне» киберсреды.

Исходя из анализа биткойна, можно утверждать, что он соотносим, скорее всего, с денежным суррогатом, который также запрещен на территории Российской Федерации. Э. С. Набиуллина подтверждает двойственное понимание Сбербанком криптовалюты. Получается, что технологии блокчейна и биткойна развиваются и не запрещены, но криптовалюта, биткойн, эфириум классифицируются как денежные суррогаты и разрешены[1].

Интересную трактовку криптовалюты можно найти в исследованиях Д. Ядрона и Б. Девлина. Они понимают биткойн, эфириум как компьютерное кодирование, характеризующееся зашифрованностью. Такие цифровые коды удобно использовать для приобретения продуктов или услуг, стоимость которых не является постоянной рыночной константой, а изменяется[2]. Таким образом, криптовалюта определяется как коды, не подверженные ни государственно-правовому регулированию, ни тем более влиянию.

В судебной практике есть прецедентное решение, когда постановление Шестого арбитражного апелляционного суда от 1 апреля 2016 года по делу № 06АП-552/2016 обязало ответчика выплатить истцу по кредитному договору вместо сингапурских долларов эквивалентную сумму криптовалютой[3]. В ГК РФ в п. 1 и п. 4 ст. 421 стороны могут заключить договор как предусмотренный, так и не предусмотренный законом или иными правовыми актами. Следовательно, при отсутствии законодательного запрета на использование криптовалюты и наличии договоренности участников договора об условиях биткойн признается объектом гражданско-правового договора, и в рамках ГК РФ сделки с криптовалютой не могут быть признаны недействительными.

---

[1] Лаборатория блокчейн Сбербанка. URL: https://www.sberbank.ru/ru/person/ promo/blockchain (дата обращения: 01.02.2019).

[2] Yadron D., Devlin B. U. S. News: Bitcoin Poses Test to Law Enforcement // Wall Street Journal. Eastern edition. New York, N.Y. 2013. 23 Oct.

[3] Постановление Шестого арбитражного апелляционного суда от 1 апреля 2016 г. по делу № 06АП-552/2016. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2021).

Таким образом, категория денежного суррогата не определена и не предусмотрена для его реализации в рамках правового поля[1]. В ГК РФ и ст. 27 федерального закона «О Центральном банке Российской Федерации (Банке России)» выявлено противоречие, поскольку при наличии договоренности участников договора об условиях биткойн признается объектом гражданско-правового договора. В то же время банковское законодательство биткойн классифицирует как денежный суррогат, запрещенный к реализации[2].

Для легализации криптовалюты необходимы изменения в Конституции, законе «О Центральном банке Российской Федерации (Банке России)», ГК РФ и КоАП РФ.

Использование криптовалюты в России предполагает изменения в законодательстве и надзор со стороны Центрального банка РФ. Однако не совсем ясны правовые основания для одновременного сосуществования в одной стране государственной и негосударственной валют.

Дискурс о легализации криптовалюты видится как более конструктивное решение по введению биткойна в рыночную систему и вывод его из «серых зон».

Исследователь П. Киаиан[3] пишет о необходимости разработки стратегии безопасности использования криптовалюты и создания надзорного органа для обеспечения надежности транзакций в системе биткойна. Возможности правового регулирования введения и обращения такой валюты должны инициировать процессы по разработке правовых дефиниций: «денежный суррогат» и «криптовалюта». После их уточнения возможно модифицировать деятельность бирж, сформулировать правовое понимание биткойна, эфириума и внести изменения в систему лицензирования банков. Обостряет ситуацию противоречие между ГК РФ и ст. 27 федерального закона от 10 июля 2002

---

[1] О Центральном банке Российской Федерации (Банке России) : федер. закон от 10 июля 2002 г. № 86-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2021).

[2] О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : федер. закон от 31 июля 2020 г. № 259-ФЗ (послед. ред.). Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2021).

[3] Ciaian P., Rajcaniova M., d'Artis K. Op. cit. P. 173 – 195.

года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», дающее возможность в финансово-банковских отношениях достаточно широко трактовать правила работы с, например, эфириумом и биткойном. В контексте такой проблематики возрастает количество судебных споров по данному вопросу.

Таким образом, в России торги с криптовалютой возможны только на зарегистрированных биржах, оформленных как юридические лица на основании федеральных законов «О рынке ценных бумаг» и «Об организованных торгах»[1], но необходима правовая регламентация правоотношений. Также следует регламентировать возможности использования криптовалюты без участия банков, что не может не вызывать обоснованные опасения об информационной безопасности этих процедур.

Правовое обеспечение блокировки деструктивной информации напрямую связано с правовым определением облачных технологий.

В соответствии с указом Президента Российской Федерации от 9 мая 2017 года № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы» облачные вычисления – «это информационно-технологическая модель обеспечения повсеместного и удобного доступа с использованием сети “Интернет” к общему набору конфигурируемых вычислительных ресурсов (“облаку”), устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными затратами или практически без участия провайдера»[2].

Международная некоммерческая организация – Институт инженеров по электротехнике и электронике (IEEE) – в 2008 году определила облачную обработку данных как «парадигму, в рамках которой информация постоянно хранится на серверах в Интернете и временно

[1] Минфин РФ опубликовал законопроект о регулировании криптовалюты. URL: https://rg.ru/2018/01/25/minfin-rf-opublikoval-zakonoproekt-o-regulirovanii-kriptovaliuty.html (дата обращения: 01.03.2020).

[2] О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы : Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собрание Законодательтства Рос. Федерации. 2017. № 20. Ст. 2901. URL: https://www.szrf.ru/ (дата обращения: 22.01.2019).

кэшируется на клиентской стороне, например на персональных компьютерах, игровых приставках, ноутбуках, смартфонах и т. д.»[1].

В «Прогнозе научно-технологического развития Российской Федерации на период до 2030 года» (утв. Правительством Российской Федерации) предусматривается создание единой информационно-технологической и коммуникационной инфраструктуры, работающей на отечественном программном обеспечении, для служащих федеральных органов исполнительной власти и государственных внебюджетных фондов, обеспечивающих предоставление государственных услуг. Анализируются возможности развития облачных сетей при трансформации программного обеспечения.

Облачные вычисления отнесены к основным сквозным технологиям[2].

В 2015 году в России распоряжением Правительства Российской Федерации от 7 октября 2015 года № 1995-р 456 была утверждена Концепция перевода обработки и хранения государственных информационных ресурсов, не содержащих сведения, составляющие государственную тайну, в систему федеральных и региональных центров обработки данных. Таким образом, необходима правовая регламентация, которая будет учитывать такие критерии, как:

– право владения;

– категории хранимой информации;

– уровни ответственности провайдера;

– функции участников облачных взаимодействий.

Концепция регламентировала возможности аккредитации, лицензирования поставщика облачных услуг. В настоящее время функционируют семь дата-центров, предоставляющих облачные сервисы для органов государственной власти и НИИ (например, создана платформа «Госприклад»).

[1] Облачные технологии. URL: https://nitforyou.com/oblachnye-texnologii/ (дата обращения: 01.02.2019).

[2] Прогноз научно-технологического развития Российской Федерации на период до 2030 года (утв. Правительством Рос. Федерации) // Собрание Законодательства Рос. Федерации. 2018. № 42 (ч. II). Ст. 6480. URL: https://www.szrf.ru/ (дата обращения: 22.01.2021).

Возникают вопросы: каким образом можно регламентировать состав облачных правоотношений? Публичный или частный фактор положить в основу правовой регламентации?

Провайдер, хостинг-провайдер, третьи лица могут выступать правообладателями ИТ в облачном хранилище.

Исследователь А. К. Жарова поясняет, что «у пользователя не возникает права собственности на используемые материальные объекты (аппаратный комплекс), он их арендует. Если пользователю предлагается к работе программное обеспечение, то такие отношения оформляются в рамках ч. 4 ГК РФ как использование результатов интеллектуальной деятельности»[1].

А. К. Жарова подчеркивает, что подобная ситуация приводит к тому, что пользователь может получить доступ к технологии, сохранить информацию в облачном хранилище, но не сможет управлять инфраструктурой облака, контролировать информационную безопасность своих данных на частном уровне.

На публичном уровне важно проанализировать риски государственного облачного хранилища. С одной стороны, государственное облако лучше защищено, но, с другой стороны, сбой в государственном облачном хранилище данных, например «Госуслуги», может привести к информационным рискам, связанным с безопасностью большого количества пользователей, использующих приложения для оплаты налогов, услуг, энергетики, медицины, образования, транспорта и разных онлайн-сервисов для оформления документов.

Пример работы в Великобритании правительственного шлюза, централизовавшего интернет-доступ к различным блокам правительственной архитектуры, – сервис Government Gateway.

1 января 2018 года введен в действие ГОСТ Р ИСО/МЭК 19831-2017. Национальный стандарт Российской Федерации. Модель и протокол интерфейса управления облачной инфраструктурой (CIMI). Интерфейс для управления облачной инфраструктурой[2], который определяет логическую модель для менеджмента ресурсов в категории «Инфраструктура как услуга» (далее – служба IaaS).

---

[1] Жарова А. К. Условия оказания услуги по предоставлению доступа к облачным вычислениям // Государство и право. 2012. № 12. С. 86 – 90.

[2] Документы в области метрологии : указатель… / Федер. агентство по техн. регулированию и метрологии ; сост.: П. К. Одинцов [и др.]. М. : Стандарт-форм, 2020. 240 с.

Таким образом, создание ГОСТа, концепций правовой регламентации позволяет сделать вывод о работе законодателя над способами правовой блокировки деструктивной информации не только в сети Интернет, но и в киберпространстве.

Вопросы и задания для самостоятельной работы

1. На чем основана система работы правового обеспечения противодействия деструктивной информации в сети Интернет?
2. Какую роль играет информационно-коммуникативная культура в организации противодействия деструктивной информации в сети Интернет?
3. Обоснуйте выбор методологии программы формирования правового противодействия деструктивной информации в сети Интернет.
4. Проанализируйте традиционные и инновационные технологии, показавшие свою эффективность в работе по противодействию деструктивной информации в сети Интернет.
5. В чем состоит роль государства в противодействии деструктивной информации в сети Интернет?
6. Какими нормативно-правовыми актами должен руководствоваться педагог, выбирая методы, формы и средства профилактики и противодействия кибертерроризму в сети Интернет?

Глава 3. ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ И СОВЕРШЕНСТВОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ В КИБЕРСРЕДЕ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ

3.1. Применение принципа интероперабельности в правовом регулировании информационных отношений в киберсреде

Приоритетное направление развития и совершенствования правового регулирования информационных отношений в киберсреде в условиях глобализации – интероперабельность, трактуемая как возможность информационных систем свободно взаимодействовать с технологиями по обмену информацией с последующей реализацией.

Производители опираются на работу с информационными системами, имеющими различное технологическое моделирование и стандартизацию. Это обусловливает опору на технологию конкретного производителя, поскольку информационные системы, организованные разными производителями, не могут работать в одном режиме. Это привносит определенные трудности в реализацию компьютерных программ и взаимодействие пользователей программного обеспечения, поскольку нивелируется взаимное открытие систем.

На современном этапе развития российского общества существует достаточное количество нормативно-правовых актов, участвующих в регулировании технологических платформ. Однако и сегодня еще не урегулирован вопрос о реализации программного обеспечения на базе открытости технологических систем. Приказом Минпромторга России от 23 июня 2016 года № 2091 «Об 565 ISO/IEC 2382 – 1:1993 Information technology – Vocabulary – Part 1: Fundamental terms»[1] утверждена Концепция развития государственной информационной системы промышленности, предусматривающая «создание единого информационного пространства взаимодействия участников ГИСП, основанного на принципах интероперабельности – способности двух или более информационных систем или компонентов к обмену информацией и к использованию информации, полученной в результате обмена – семантической интероперабельности» (п. 2.3). На

[1] Об 565 ISO/IEC 2382 – 1:1993 Information technology – Vocabulary – Part 1: Fundamental terms : Приказ Минпромторга России от 23 июня 2016 г. № 2091. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2020).

основе концепции структура государственной информационной системы промышленности (ГИСП) к 2021 году стала включать управление нормативно-справочной информацией и обеспечивать взаимодействие ГИСП с информационными структурами, опираясь на семантическую способность систем обмениваться информацией. Государственно-информационная система прошла определенный филогенез, включающий «комплекс управления нормативно-справочной информацией и обеспечения информационного взаимодействия ГИСП с внешними информационными системами на базе семантической интероперабельности» (п. 8)[1]. Высший Евразийский экономический совет 11 октября 2017 года утвердил Положение № 12 «Об основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года»[2], основной целью которого выступил симбиоз информационных потенциалов государств-членов, обеспечивающий существенный уровень открытых информационных систем.

В ГОСТ Р ИСО 21091-2017. Национальный стандарт Российской Федерации. Информатизация здоровья. Службы каталога поставщиков и субъектов медицинской помощи и других сущностей (утв. приказом Росстандарта от 21 июня 2017 года № 570-ст 569) определен ряд требований к технологической открытости информационных систем: «Каталоги, предназначенные для здравоохранения, должны иметь возможность контактировать с каталогами различных деловых партнеров и/или взаимно обмениваться с ними информацией. Для этих целей используются такие методы, как связывание в цепочки, репликация, отправка данных, а также формирование одностороннего или двустороннего доверия между каталогами. В зависимости от приложения или службы некоторые из этих методов будут чувствительными к несогласованности схем»[3].

---

[1] Жарова А. К. О правовом регулировании технологического обеспечения информационного взаимодействия субъектов // Труды Института государства и права. 2012. № 3. С. 186 – 199.

[2] Положение № 12 «Об основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2020).

[3] ГОСТ Р ИСО 21091-2017. Национальный стандарт Российской Федерации. Информатизация здоровья. Службы каталога поставщиков и субъектов медицинской помощи и других сущностей : утв. приказом Росстандарта от 21 июня 2017 г. № 570-ст 569. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2020).

Указанный документ обозначил требования, необходимые для технологической открытости систем: опора на программные интерфейсы, реализуемые на всех уровнях информационных систем, – это один из значимых путей обеспечения обмена информацией. Анализируя возможные направления развития экономических отношений, следует обратиться к интероперабельности как необходимому условию, обеспечивающему использование информационных технологий. Достаточно часто пользователи задаются вопросом: возможна ли разработка информационных технологий, не учитывающих принцип интероперабельности? Теоретически такое положение возможно. Практически же это вызовет проблемы во взаимодействии самых разных технологических платформ и ограничит совершенствование информационного общества в целом, а также усложнит организацию успешного государственного управления, базирующегося на применении различных информационных технологий.

Введенный в Российской Федерации интегративный блок стандартов ИСО 16100 обеспечивает решение следующих проблем:

а) постоянно увеличивающуюся базу решений, зависящих от поставщиков;

б) трудности применения стандартов;

в) переход к модульным наборам инструментальных средств интеграции системы;

г) способность физически разделить базу/сообщество клиентов здравоохранения на контролируемые компоненты, предоставляющие развитые службы;

д) способность обеспечить репликацию и управление балансировкой нагрузки;

е) способность ограничивать дерево поиска до конкретной географической или логической области;

ж) способность организовать дерево информации каталога таким образом, чтобы разрешения доступа относились к точкам ветвления;

з) способность организовать дерево информации каталога таким образом, чтобы можно было обеспечить распределенный доступ к региональной информации системы здравоохранения[1].

[1] ГОСТ Р ИСО 16100-6-2014. Национальный стандарт Российской Федерации. Системы промышленной автоматизации и интеграция. Профилирование возможности интероперабельности промышленных программных средств. Часть 6. Службы и протоколы интерфейса для сопоставления профилей, основанных на многоцелевых структурах классов возможностей : утв. приказом Росстандарта от 26 нояб. 2014 г. № 1871-ст. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2020).

Представленный в ГОСТ Р ИСО 16100-6-2014 «Системы промышленной автоматизации и интеграция. Профилирование возможности интероперабельности промышленных программных средств. Часть 6. Службы и протоколы интерфейса для сопоставления профилей, основанных на многоцелевых структурах классов возможностей» пакет нормативных документов ориентирован на создание цифровых ресурсов, определяющих возможный формат цифровых технологий, интерпретируемых компьютером в электронно-цифровой форме, реализацию программ и детерминирующих выбор методологии для анализа значимых способностей программ, обеспечивающих их успешность в промышленном цикле, исходя из витального цикла производства, архитектоники системы или совершенствующейся информационной платформы.

Основной структурный компонент реализации ИКТ-политики – интероперабельность информационных инфраструктур, разрабатываемая во многих государствах на протяжении последнего десятилетия. Примером может служить Европейское агентство сетевой и информационной безопасности (ENISA – European Network and Information Security Agency), отразившее в своем отчете «Электронные удостоверения личности» проблемы, связанные с технологической открытостью информационных технологий, селекцией стандартов, взаимодействием информационных технологий, отличающихся по содержательной фабуле, обеспечивающих трансформацию данных вкупе с их безопасностью, а также отождествление и аутентификацию пользователей.

Невозможно решить проблемы, связанные с обеспечением безопасности информационных технологий, если не задаться вопросом о разработке нормативной базы и определении политик безопасности разного уровня. В Российском государстве такая работа ведется с 2009 года. В частности, в утвержденном постановлении Правительства Российской Федерации от 3 октября 2009 года № 796 «О некоторых мерах по повышению качества предоставления государственных (муниципальных) услуг на базе многофункциональных центров предоставления государственных (муниципальных) услуг» раскрыта дефиниция интероперабельности при разработке протоколов передачи структур классов возможностей и других информационных технологий.

Необходимо отметить, что ряд документов, принятых по организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг, сегодня уже не отра-

жают всей полноты открытости системы. Правила 2012 года определяли, что задача многофункционального центра – использование автоматизированной системы, обеспечивающей взаимодействие с такими государственными направлениями, как федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме», Единая система межведомственного электронного взаимодействия, Региональная система межведомственного электронного взаимодействия; автоматизированная информационная система «Информационно-аналитическая система мониторинга качества государственных услуг», Государственная информационная система о государственных и муниципальных платежах. В ст. 21 федерального закона от 27 июля 2020 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» указано, что названные системы функционируют таким образом, чтобы была возможна их взаимная интеграция в случае их «открытости».

Информационные системы, содержащие данные в разных форматах, находятся в уязвимом положении. Даже при наличии инструкций, которые были направлены на регламентацию обеспечения максимально безопасного (удобного) доступа к разным формам ресурсов, учитывая возможности/запреты пользователей с разными уровнями доступа к информационным данным, сохранялась возможность получения данных третьими лицами.

Уровень технического развития и информационного насыщения «серой зоны» даркнет инициирует дополнение «Правил организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг»[1] (утв. постановлением Правительства Российской Федерации от 22 декабря 2012 г. № 1376). Это следует из анализа категорий открытости и их возможностей для информационных рисков стратегии безопасности Российской Федерации. Многофункциональный центр, деятельность которого описана в

[1] Об утверждении Правил организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг : постановление Правительства Рос. Федерации от 22 дек. 2012 г. № 1376 (ред. от 27 нояб. 2021 г.). Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения 28.11.2021).

правилах 2012 года, опирается на технологии автоматизации и макровзаимодействие одной системы с другими государственными информационными системами (Госуслуги, Информационно-аналитическая система мониторинга качества государственных услуг, Единая система идентификации и аутентификации в инфраструктуре, обеспечивающие информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме, и др.). Принцип открытости этих систем является условием их работы. В то же время принцип открытости многофункционального центра нуждается в дополнении принципами валидности пользователей, постоянном мониторинге провайдеров, которые никаким образом не зарегистрированы в ведомстве национальных правовых систем.

Сегодня регистрация провайдера и собственника IP адреса по месту реального проживания представляет собой серьёзную проблему, которая вынуждает законодателя искать новые пути и возможности идентификации пользователей. Фактор глобализации допускает возможности для иностранного гражданина получать полный доступ к открытым многофункциональным системам.

С 2012 по 2021 год законодатель проводил работу над поиском путей по выявлению идентификации иноагентов, в частности newsmakers в СМИ России, продолжая поступательную доработку закона № 121-ФЗ[1]. Аналогичная правовая инициатива осуществляется с 1939 года в США (FARA).

Открытость информационных многофункциональных систем должна способствовать превенции рисков. Необходима четкая система регламентации деятельности НКО, получающей денежные средства, имущество от иностранных государств, иностранных граждан, лиц без гражданства либо уполномоченных ими лиц, ведущих деятельность не в интересах Российской Федерации на территории нашей страны.

Концепция формирования механизма публичного представления предложений граждан Российской Федерации с использованием ин-

[1] О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента : федер. закон от 20 июля 2012 г. № 121-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2020).

формационно-телекоммуникационной сети «Интернет» (утв. Правительством Российской Федерации) определяет важные принципы для информационной безопасности:

1) открытости;
2) законности;
3) обязательности рассмотрения;
4) доступности (в частности, для лиц с ОВЗ).

Процедурно в концепции определяется регламент правовой инициативы, правового предложения. В соответствии с процедурой вырабатывается иерархия рабочих групп, которые проводят анализ и экспертизу. «Поддержанным считается предложение, которое в течение одного года после его размещения с использованием специализированного ресурса собрало 100 тыс. голосов и более “за”. Предложение, не набравшее в течение одного года 100 тыс. голосов “за”, считается не поддержанным и снимается с голосования»[1]. Такая политика законодателя направлена на развитие взаимодействия со всеми социальными структурами и Правительством Российской Федерации.

В то же время законодатель четко определяет вопросы, которые не могут выноситься на референдум в соответствии со ст. 5 федерального конституционного закона от 28 июня 2004 года № 5-ФКЗ (ред. от 30 декабря 2021 года) «О референдуме Российской Федерации».

Концепция предусматривает, что взаимодействие должно строиться на основе принципов открытости информации и интероперабельности, понимаемых как способности интегрировать ИКТ ресурсы.

Цифровизация, затрагивающая все сферы человеческого бытия, при осмыслении футурологической наукой тяготеет к применению «умных» технологий, появлению новых тенденций к улучшению личной эффективности с помощью ИТ технологий как отдельно взятой личностью, так и транснациональными корпорациями. Этот процесс остановить невозможно. Интенсивное совершенствование экономического сектора сегодня значительно опережает развитие правового его осмысления. Так, например, в Японии существуют туристические организации, где все операции осуществляют роботы, однако

[1] Концепция формирования механизма публичного представления предложений граждан Российской Федерации с использованием информационно-телекоммуникационной сети «Интернет» для рассмотрения в Правительстве Российской Федерации предложений, получивших поддержку не менее 100 тыс. граждан Российской Федерации в течение одного года : утв. Правительством Рос. Федерации. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2020).

статус робота, классификации роботов не описаны ни в одном правовом документе и не контролируются никакими нормативно-правовыми актами, кроме как, например, ГК РФ, в качестве собственности.

В Москве уже сегодня есть роботы-такси, которые могут сбиться с маршрута или попасть в аварию. Ситуацию, когда в аварию попадает транспортное средство, управляемое принадлежащей собственнику ИТ, роботом, кибернетической системой с ИИ, – прецедентная ситуация с точки зрения права.

Современная правовая действительность опирается на регламентацию существующих и растущих технологий ИКТ в области, например, организации электронных платежей в глобальном их понимании. Разработанная «Стратегия развития национальной платежной системы на 2021 – 2023 годы» (утв. Банком России) направлена на поиск интегративных аспектов для проведения дифференцированных платёжных операций. Примером зарубежной политики в этом вопросе может служить применение международного стандарта ISO 20022, регламентирующего, например, структуру, формат электронного финансового сообщения.

Таким образом, интероперабельность сегодня включает в себя три критерия: глобальный, организационный, технический. Высокий интерес к интероперабельности имеет помимо экономического и военный сектор.

В ЕС отдел по разработке профилей интероперабельности Board Interoperability Profi les Capability Team – IP CaT постоянно дорабатывает документ «Стандарты и профили интероперабельности НАТО» (NATO Interoperability Standards and Profiles – NISP). В России информации об аналогичном документе в СПС «КонсультантПлюс», «Гарант» – нет[1], но ведется активная работа по его созданию. Об этом свидетельствуют с 2011 года 27 приоритетных технологических платформ, утверждённых Правительством Российской Федерации[2].

---

[1] Олейников А. Я., Чусов И. И. Проблема интероперабельности в Вооруженных силах РФ // Вестник Академии военных наук. 2017. № 4 (61). URL: http://www.avnrf.ru/index.php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov/1044-vestnik-avn-4-2017 (дата обращения: 15.01.2020).

[2] IDBC. URL: http://ec.europa.eu/idabc/servlets/Doca2cd.pdf (дата обращения: 19.01.2021) ; Труды Пятой Всероссийской конференции. Стандартизация информационных технологий и интероперабельность. СИТОП. 2011. URL: http://www.sitopconf.ru/files/sitop2011.pdf (дата обращения: 19.01.2021) ; Протокол заседания Правительственной комиссии по высоким технологиям и инновациям от 1 апреля 2011 г. № 2. URL: http://www.hpc-platform.ru/tiki-download_file.php?Fileid=38 (дата обращения: 19.01.2021).

Под технологической платформой законодатель понимает «коммуникационный инструмент, направленный на активизацию усилий по созданию перспективных коммерческих технологий, новых продуктов (услуг), на привлечение дополнительных ресурсов для проведения исследований и разработок на основе участия всех заинтересованных сторон (бизнеса, науки, государства, гражданского общества), совершенствование нормативно-правовой базы в области научно-технологического, инновационного развития»[1].

В 2016 году приказом Росстандарта от 22 апреля 2016 года № 463 в структуру ТК-22 (технического комитета по стандартизации «Информационные технологии») введен подкомитет ПК 206 «Интероперабельность». Такое решение законодателя следует понимать как усиление технического регулирования информации в киберсреде. Сегодня важно осознавать, что необходима интегративная инфраструктура, которая позволит применить интероперабельность в самых дифференцированных схемах, не выходя за пределы информационной безопасности. Разработка и функционирование non-custodial кошельков может децентрировать управление большим количеством активов, например финансовых, пользователем в самых разных сетях, информационных структурах киберсети легально. Примером попытки внедрения интероперабельности в блокчейн-системы служит внедрение кроссчейн-кошелька XDefi[2].

В 2017 году в состав ТК-22 Росстандартом введен технический комитет по стандартизации «Кибер-физические системы» (ТК-194)[3]. Планировалось, что комитет выработает национальные стандарты, частично интегрируя их с международными, чтобы была возможность соприкосновения при составлении международно-правовых договоров.

---

[1] Утв. решением Правительственной комиссии по высоким технологиям и инновациям от 3 авг. 2010 г., протокол № 4583. П. 2.

[2] Солодков А. «Интероперабельность выгодна всем, автономные блокчейны не нужны никому» : интервью с Ником Аврамовым, сооснователем Symbiosis Finance. 2021. URL: https://bloomchain.ru/people/interoperabelnost-vygodna-vsem-avtonomnye-blokcheiny-ne-nujny-nikomu-intervju-s-nikom-avramovym-soosnovatelem-symbiosis-finance (дата обращения: 01.02.2021).

[3] Shaik M. H., Kamaludin M. Y., Shaik A. H., Eberechukwu N. P. A Review of Interoperability issues in Internet of Vehicles (IoV) // International Journal of Computing and Digital Systems. 2019. Vol. 8. No. 1. Pp. 73 – 83.

В приказе от 27 марта 2017 года № 642 «О создании технического комитета по стандартизации «Кибер-физические системы» (с изм. от 24 апреля 2024 года) в целях реализации федерального закона № 162 от 29 июня 2015 года «О стандартизации в Российской Федерации» законодатель дает возможность создания рабочих групп: «Интернет вещей и цифровые двойники» (РГ1), «Умные города и умные дома» (РГ2), «Умное производство» (РГ3), «Квантовые технологии» (РГ6), «Нейротехнологии и нейроинтерфейсы» (РГ9) и др. [1]

Включение в ИТ-разработки подобных ГОСТов создаст правовую основу для надзора за предупреждением развития деструктивной информации в киберинформационной среде, которая сегодня находится в «серой зоне» и для которой не существует единых правовых норм, способных противодействовать ее влиянию.

Исследователи А. Я. Олейников, И. И. Чусов определили структуру эталонной модели интероперабельности (рис. 2).

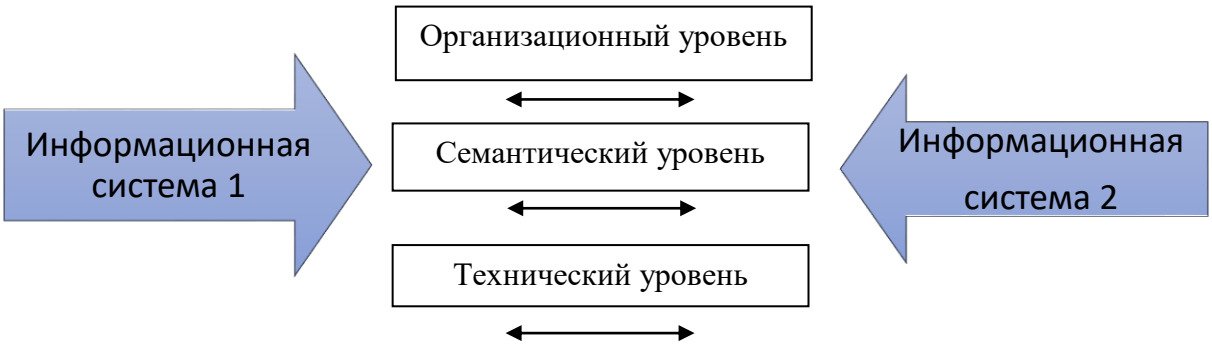

Рис. 2. Эталонная модель интероперабельности[2]

[1] ГОСТ Р «Умный город. Эталонная структура ИКТ. Часть 1. Структура бизнес-процессов Умного города» (гармонизация с ИСО/МЭК 30145-1); Часть 2. Структура управления знаниями Умного города (гармонизация с ИСО/МЭК 30145-2) ; Часть 3. Инженерные системы Умного города (гармонизация с ИСО/МЭК 30145-3)) ; ГОСТ Р «Интернет вещей. Эталонная архитектура» (гармонизация с ИСО/МЭК 30141) ; ГОСТ Р «Интернет вещей. Интероперабельность систем “Интернета вещей”». Часть 1. Структура» (гармонизация с ИСО/МЭК 21823-1) ; ГОСТ Р «Интернет вещей. Интероперабельность систем “Интернета вещей”». Часть Х. «Семантическая интероперабельность» (гармонизация с ИСО/ МЭК 21823-Х) ; ГОСТ Р «Большие данные. Эталонная архитектура» (гармонизация с ИСО/МЭК 20547) ; ГОСТ Р «Большие данные. Термины и определения» (гармонизация с ИСО/МЭК 20546) Башлыкова А. А., Олейников А. Я., Гаджикулыев Т. А. Решение проблемы интероперабельности в проектах «Умного города» // Современные информационные технологии и ИТ-образование. 2019. V. 5. № 3. DOI: 10.25559^тТО. 15.201903.767-774.

[2] Олейников А. Я., Чусов И. И. Указ. соч. С. 63.

Принцип интероперабельности, положенный в основу информационной безопасности, позволяет говорить о необходимости выработки семантического уровня, определения и уточнения прав и обязанностей провайдера в киберсети, аналогично с пониманием персональных данных.

Приоритетные пути регулирования вредной киберинформации в сети Интернет составляют важную исследовательскую линию в юридической технике в условиях глобализационного фактора.

Сегодня очевидно, что тот, кто управляет информационной структурой в «серой зоне», может влиять на государственную, экономическую, военную и личную безопасность.

Информация сама по себе нейтральна, но высока ее возможность к интерпретации, трансформации через симулякративные смыслы. Психологичность и внутренняя семиотичность делают ее оружием в руках человека с деструктивными намерениями. Киберинформационная сеть, включающая в себя Интернет и киберсреду, долгое время находится в противоречивом положении (разные нормативные акты в международном блоке взаимоисключают друг друга). Такая ситуация породила правовой нигилизм, реагирование на информацию без ее следственно-причинного анализа, снижение критического мышления у молодежной категории пользователей.

Информация в современной киберсреде доступна, управляема как государством, так и частными лицами. Не нужны специальные навыки, чтобы стать пользователем любого приложения, ИТ. В то же время созданные ИТК позволяют выявлять вредную информацию, удалять ее, блокировать, предотвращать ее распространение.

Интероперабельность как принцип сложно реализовать без привлечения провайдеров хостовых услуг (информационных посредников).

Под информационным посредником законодатель может подразумевать и провайдера, и провайдера хостовых услуг, и лиц, оказывающих в сети Интернет услуги операторов, связывая их деятельность с гражданским оборотом результатов интеллектуальной собственности и деятельности. Таким образом, провайдер обеспечивает хост, информационную структуру, используя которую субъекты могут получать, распространять, удалять информацию, а следовательно, провайдер может этот процесс контролировать и пресекать правона-

рушения. Сложный дискурс выявляется при осознании, что субъекты могут быть гражданами разных государств, т. е. ответственность за любое правонарушение интернет-пользователя в отношении каждого государства нужно будет выстраивать исходя из интеграции национального и международного права. Примеры подобной сложности – распространение субъектом деструктивной информации и отказ ее удалять. В таком случае необходимо понимать, каким образом данная деструктивная информация может быть удалена как нарушающая национальное законодательство.

Практика международных соглашений показывает дифференцированный подход к этой ситуации, который детерминируется политической ситуацией или отсутствием технических средств.

Исследователь А. К. Жарова выделяет шесть типов провайдеров:

1) провайдеры содержания (контент);
2) провайдеры хостовых услуг;
3) провайдеры доступа;
4) сервис-провайдер (с 2012 года (в зарубежной практике));
5) удостоверяющий провайдер (с 2012 года (в зарубежной практике));
6) идентифицирующий провайдер (с 2012 года (в зарубежной практике))[1].

Зарубежные исследователи отводят значительную роль провайдеру, который размещает информацию для предупреждения правонарушений в «серой зоне»[2].

Интересно представить систему действий провайдера в случае наступления юридической ответственности. В отечественной юридической теории необходимо уточнить вектор понимания юридической ответственности и функций провайдера.

Исходя из приведенной выше классификации определяются границы ответственности: так, провайдеры содержания модерируют принадлежащий им информационный контент, провайдеры хостовых

[1] Жарова А. К. Информация. Правовые проблемы обращения информации. М., 2006. С. 134.

[2] The National Strategy for Trusted Identities in Cyberspace of USA, 2011; The Identity Assurance Programme of UK, 2014. URL: https://www.nao.org.uk/wp-content/uploads/2014/12/Identity-Assurance-Programme1.pdf (дата обращения: 14.12.2019).

услуг регулируют ИТ, ИТК на технологическом уровне на основе гражданского договора, а сам хостинг определяется Директивой Европарламента и Совета ЕС 2000/31/ЕС об электронной коммерции[1].

В то же время хостинг-провайдер не контролирует информацию в отличие от провайдера содержания, так как предоставляет облачное хранилище для конфиденциальной частной информации, и на основе закона о персональных данных это будет правонарушением. Электронная почта, социальная сеть – все это модерируется хостовым провайдером. В то же время ISP (интернет-провайдеры), являющиеся организациями, которые предоставляют доступ к интернет-инфраструктуре, не осуществляют мониторинг, модерацию информации, которая выкладывается пользователями их услуг. Вредная кибериинформация может находиться в информационной инфраструктуре до того момента, пока она не признана деструктивной. Тогда, согласно ч. 4. «Закона об информации», она должна быть удалена провайдером по запросу правоохранительных органов, опирающихся на реестры вредной, деструктивной, противозаконной информации, классифицируемой на основе решений судов в Российской Федерации.

Есть провайдеры, которые предоставляют доступ к интернет-технологиям, не контролируя информацию, которая будет распространяться.

Риски связаны с информацией, размещенной на международных платформах. Ее нельзя удалить, опровергнуть, заблокировать. Поэтому принятие и доработка федерального закона № 121 выступают превентивным инструментом[2].

Федеральный закон «Об информации» (ч. 3 ст. 17) предполагает гражданско-правовой вид ответственности за распространение запрещенной, искажение частной или конфиденциальной информации. Таким образом, законодатель предусматривает наличие ответственности за ненадлежащее применение информации не только блогером, провайдером, но и участником информационных правоотношений

[1] Жарова А. К. Информация. Правовые проблемы обращения информации. М., 2006. С. 135.

[2] О внесении изменений в отдельные законодательные акты Российской Федерации в части регулирования деятельности некоммерческих организаций, выполняющих функции иностранного агента : федер. закон от 20 июля 2012 г. № 121-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2020).

(пользователей киберсети). Лица, которые сознательно нарушают требования информационной безопасности в отношении хранения, распространения, искажения (например, биометрических данных), могут нести административную, уголовную и гражданскую ответственность.

В международно-правовой практике наблюдается двойственное отношение к этой ситуации: например, в законе КНДР «О компьютерной информационной сети и интернет-безопасности, защите и управлении»[1] указано, что провайдеры должны выявлять, ставить специальные компетентные органы в известность о размещении конкретным IP-адресом подобной информации, ограничивать доступ к вредным источникам информации в Интернете.

Информационную безопасность в сети Интернет в киберинформационном пространстве невозможно обеспечить с помощью правовых ресурсов одного государства. Сегодня это стало общей межгосударственной задачей, поэтому в ЕС, например, предпринимается попытка ввести рейтинговую систему по оценке элементов информационной структуры, чтобы выявлять максимальное количество опасных ресурсов (Кодекс поведения в Интернете). В то же время ситуация с ответственностью провайдера за обнаружение деструктивной и вредной киберинформации все также не ясна, предусмотрена регламентация ее удаления на основании рейтинга или обращения компетентных структур.

Сегодня на международном уровне законодатель определил правовое регулирование как уровень ответственности за наличие на ресурсе вредной киберинформации. В Российской Федерации, США, ЕС, Великобритании выработана аналогичная стратегия. При выявлении деструктивной составляющей информации ее необходимо удалить, устранить, заблокировать, если, например, она относится к серверу другой страны, но признать ее деструктивной в правовом определении не представляется возможным. Важным условием выступает форма извещения провайдера о проблеме.

Сложную правовую ситуацию создают пользователи proxy-сервера, поскольку он выступает промежуточным комплексом про-

[1] Computer Information Network and Internet Security, Protection and Management Regulations, 1997 г. URL: http://www.qis.net/chinalaw/prclaw54.htm (дата обращения: 15.01.2020).

грамм, посредником между, например, гаджетом и итоговым сервером. С одной стороны, proxy-сервер повышает конфиденциальность пользователя, позволяет отражать кибератаки, но, с другой стороны, он также выступает средством злонамеренного причинения вреда мошенниками для сокрытия в кэше вредной ссылки, перехвата частных данных, например финансовых; с его помощью можно обходить блокировки ресурсов, пользуясь региональными разрешениями, и изменить в киберсреде свой IP.

В Российской Федерации 13 сентября 2021 года «Ростелеком» запретил применение публичных DNS-серверов Google, Cloudflare и сервиса DoH (doh.opendns.com)[1]. В других странах вводятся аналогичные требования к провайдерам хостинга о блокировке proxy-серверов, удалении информации третьих лиц, например размещенной на досках объявлений, если компетентными органами признано, что выявлен факт нарушения закона.

Сегодня не существует единых стандартов, которые могли бы удешевить поиск IP, с которых ведется деструктивная, преступная деятельность. В то же время есть прецедентные решения судов, обращающих внимание на действия провайдера. Так, в деле Центра религиозных технологий против Netcom On-Line Communication Services Inc. (1995) суд квалифицировал отказ провайдера в блокировании РИД при доказанном нарушении интеллектуальных прав как создание условий для правонарушения[2]. Суд не смог принять решение без судебного разбирательства по факту косвенной ответственности провайдера за нарушение авторских прав подписчиком и за то, что не была удалена некорректно размещенная информация, нарушающая авторское право.

С 1 января 2004 года в Российской Федерации был введен ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (утв. постановлением Госстандарта Российской Федерации от 4 апре-

[1] «Ростелеком» запретил использование публичных DNS-серверов Google, Cloudflare и сервиса DoH. URL: https://www.tadviser.ru/ (дата обращения: 16.11.2021).

[2] Religious Technology Center v. Netcom. URL: http://www.loundy.com/CASES/RTC_v_Netcom.html (дата обращения: 15.01.2020).

ля 2002 года № 133-ст)[1]. В документе представлены механизмы сертификации, стандарты, система требований, критериев для анализа ИТ-ресурсов.

Таким образом, нормативно-правовые акты в Российской Федерации констатируют необходимость использования полученных результатов для корректировки нормотворчества и правоприменения в области правового регулирования деятельности информационных посредников, их ответственности за способы использования информации и размещаемые на их сервере информационные ресурсы. Киберсреда транснациональна и нуждается в создании централизованного киберправа, уточнении и правовом осмыслении новых цифровых феноменов.

По состоянию на сегодняшний день федеральный закон от 27 июля 2006 года № 149-ФЗ (ред. от 30 декабря 2021 года) «Об информации, информационных технологиях и о защите информации» не предусматривает достаточного количества правовых инструментов упорядочивания процедуры правового регулирования информационных отношений в киберсреде, блокировки деструктивного контента.

В качестве возможного средства преодоления указанного недостатка можно назвать разработку и внедрение механизма выявления вредной киберинформации. Для этого необходимо повысить технологическую открытость, легальность, упорядочить процедуру сертификации киберпространства. При этом важно учитывать, что должностные лица, которые принимают решения, могут находиться в межгосударственном, транснациональном пространстве, в котором влиять на содержание и механизмы формирования правовой нормы будут национальные системы правовых доктрин.

Сегодня практика работы международных организаций по созданию информационной инфраструктуры в трансграничной концепции не всегда может эффективно и своевременно преодолеть политические и технологические разногласия для эффективного правового

[1] Государственный стандарт РФ ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» : утв. постановлением Госстандарта Рос. Федерации от 4 апр. 2002 г. № 133-ст. Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.02.2020).

управления деструктивными явлениями киберсреды. Таким образом, выработка определённых соглашений по регулированию информационных отношений нуждается в уточнении способов юридико-технической работы по созданию нормативно-правового акта: написанию, внесению изменений, редактированию и т. д. Перед законодателем стоит сложная задача поиска новых путей процессуального регулирования блокчейн-технологий, кибервалюты, информационной государственной многофункциональной телекоммуникационной инфраструктуры, частных облачных хранилищ, прокси-серверов, IOT, IT в киберинформационной системе.

Информация представляет собой сложную дифференцированную поливалентную систему, имеющую сложную, не всегда взаимообусловленную структуру. Таким образом, информация может трактоваться исходя из ее конструктивного и деструктивного потенциалов.

В. Н. Лопатин объясняет, что вредная информация «не является конфиденциальной, но ее распространение и применение через сети коммуникаций наносят вред человеку, обществу и государству»[1]. Следовательно, при наличии вредной информации говорят о деструктивных информационных ресурсах, вредном софте, программном обеспечении, ИИ и т. д. Появление такой деструктивной информации может сформировать самые сложноструктурные риски в виде цифровой преступности, киберпреступности, кибертерроризма.

Исследователи С. В. Дьяков, В. Н. Лопатин, И. М. Мацкевич выделяют следующие элементы вредной киберинформации:

1. Деструктивные идеи, унижающие честь, достоинство как отдельной личности, так и социальных групп, отдельных этносов, конфессий.

В ст. 29 ч. 2 Конституции Российской Федерации постулируется, что «не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть и вражду. Запрещается пропаганда социального, расового, национального, религиозного или языкового превосходства». В ст. 9 федерального закона № 95-ФЗ «О политических партиях», ст. 16 федерального закона № 82-ФЗ «Об общественных объединениях», ст. 48 федераль-

[1] Лопатин В. Н. Проблемы правовой защиты человека в информационной войне // Информационное право. 2014. № 6 (42). С. 18.

ного закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации», а также в ч. 1 ст. 282 УК (действия, направленные на возбуждение ненависти либо вражды, а также унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, а равно принадлежности к какой-либо социальной группе, совершенные публично или опираясь на информацию социальных институтов) констатируется правонарушение, предусмотренное ст. 1 федерального закона № 114-ФЗ «О противодействии экстремистской деятельности». В ст. 6 федерального закона № 80-ФЗ «Об увековечении победы советского народа в Великой Отечественной войне 1941 – 1945 годов» законодатель подчеркивает, что необходимо принимать меры по предотвращению распространения фашизма, фашистских организаций, в том числе в киберсреде. Сущность социальных норм любого демократического государства, и Российская Федерация не является исключением, состоит в том, что уголовной ответственности подвержены любые действия, направленные на упоминание деструктивной семиотики как унижающей честь и достоинство народов России, пострадавших от фашистского ига, а также оскверняющие память о воинах, жертвах Великой Отечественной войны.

2. Уголовному преследованию подвергаются лица, экстремистская деятельность которых направлена на нивелирование основополагающих человеческих ценностей, распространение действий, предполагающих разрушение конституционного строя государства, мародерство, массовые беспорядки. В январе 2022 года весь мир наблюдал за событиями в Казахстане, когда по приказу террористов из Афганистана и Сирии были захвачены телекоммуникационные центры, отделы полиции, банки и прочие объекты инфраструктуры. Большое количество жертв среди мирного населения, полиции, обезглавливание людей свидетельствовали о бесчеловечном поведении террористов, пытавшихся свергнуть государственную власть Казахстана.

Анализируя данную ситуацию, президент Белоруссии А. Лукашенко отметил, что цель подобных действий – разрушить Россию, подорвать ее изнутри, чтобы ослабить ее границы и суверенитет.

Статья 68 федерального закона «О референдуме» четко констатирует, что любые митинги, собрания, встречи, разрешенные государ-

ственными структурами, не должны пропагандировать терроризм, национализм, шовинизм, насилие, агрессивность, любые деструктивные действия. В противном случае лица, нарушившие федеральные законы № 5-ФЗ «О референдуме Российской Федерации» и № 35-ФЗ «О противодействии терроризму», будут привлечены к уголовной ответственности на основании (ст. 205, а также ст. 15.3 закона об информации).

Таким образом, в интегрированной киберинформационной среде трудно установить единообразное понимание правового вреда для человека, позиционирующего себя в своей деятельности как гражданина всех государств, гражданина мира, который использует право так, как выгодно ему, опираясь на разное понимание ряда правовых категорий в национальном праве разных государств.

3. Негативные процессы, происходящие в различных государствах по вине человека, несут вред каждому гражданину, социальной общности независимо от этнической и конфессиональной принадлежности. В учебном пособии представлен анализ вреда, приносимого распространением недостоверной информации, скрывающей истинное положение дел. Основываясь на федеральном законе от 27 декабря 1991 года № 2124-1 «О средствах массовой информации», можно сказать, что недопустимо «сокрытие или фальсификация общественно значимых сведений, распространение слухов под видом достоверных сообщений». Продолжают действовать ст. 8 и 11 федерального закона от 30 марта 1999 года № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения»; ст. 5 – 7 федерального закона от 10 января 2002 года № 7-ФЗ «Об охране окружающей среды»; ст. 13 федерального закона от 09 февраля 2009 года № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»; ст. 6 федерального закона от 21 декабря 1994 года № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», предусматривающие административное наказание за фальсификацию информации, имеющей важное значение для сохранения здоровья населения страны. В ст. 8.5 КоАП РФ зафиксирована ответственность за сокрытие или искажение экологической информации. В ст. 237 УК РФ отмечается, что за сокрытие или искажение ин-

формации о событиях, фактах или явлениях, создающих опасность для жизни или здоровья людей либо для окружающей среды, лицом, обязанным обеспечивать население указанной информацией, также предусмотрено наказание.

Таким образом, дефиниция «вредная киберинформация» нуждается в определении в контексте современной правовой проблематики. Законодатель акцентирует внимание на состоянии информационной инфраструктуры в киберинформационных транснациональных отношениях. Правовое определение состояния киберсреды детерминировано неопределенностью. Статья 10 закона об информации определяет ответственность за информационный контент, например, для блогеров. В ситуации перенасыщенности информационными потоками киберсреды важен контроль за фальсифицированной, невалидной информацией, но еще более острую полемику вызывают способы ее удаления. Законодатель определяет ответственность как блогеров, так и провайдеров за распространение вредной информации, ее хранение, удаление, размещение.

4. Законодатель запретил распространение текстов, идущих вразрез с нормами не только права, но и морали, афиширование порнографических материалов, нецензурной лексики в местах проживания этноса, а также при публичном чтении художественной литературы, трансляции произведений искусства на культурно-просветительских мероприятиях. Административной ответственности подвержены лица, публично демонстрирующие акты вандализма, маргинальности, нецензурные образы, унижения представителей отдельных этносов, пола, конфессий, социальных групп, государственной и религиозной символики, объектов, входящих в культурное наследие Российской Федерации и включенных в Список всемирного наследия.

5. Незнание законов не освобождает индивидов от ответственности, поэтому рекламу психоактивных веществ, разрушающих здоровье, необходимо удалять, а человек, осуществивший это деяние, должен быть подвергнут административной ответственности.

Превентивная работа сегодня исходит из создания ИТ-, ИИ-ресурсов для своевременного выявления деструктивных последствий для физического, психического и социального здоровья и статуса ин-

дивида. Например, федеральный закон № 38-ФЗ от 13 марта 2006 года «О рекламе», ст. 15.1 федерального закона об информации.

В п. 8 ст. 7 закона «О рекламе» также предусмотрено наказание за распространение спиртосодержащих изделий и никотиновой продукции.

6. Призывы к суициду, особенно в отношении несовершеннолетних, подвергаются уже уголовному преследованию. В качестве примера можно привести распространенную недавно в Интернете группу «Синий кит», в которой подростков программировали на самоубийство, играя на их возрастных и физиологических особенностях. Организатор этой игры был изобличен и предстал перед судом.

Федеральный закон от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» предусматривает достаточно жесткое наказание за популяризацию деструктивной информации среди несовершеннолетних, поскольку криминализованные элементы, пользуясь социальной незрелостью, доверчивостью и эпатажностью несовершеннолетних, склоняют их к действиям, носящим делинквентный, суицидальный и маргинальный характер. Поэтому государственные структуры, институты воспитания и социализации обязаны не только защитить детей от информационного произвола, но и обучить их дифференцированному подходу к любому инфоагенту.

Таким образом, анализ критериев деструктивной информации, способной оказать потенциально разрушительное воздействие, обусловливает введение новой дефиниции «вредная киберинформация» в законодательство Российской Федерации. В соответствии с п. 4. ст. 5 закона «Об информации, информационных технологиях и о защите информации» необходимо дополнить классификацию, расширив понятие информации, «распространение которой ограничивается или запрещается», дефиницией «вредная киберинформация».

Не менее сложен вопрос, касающийся возможностей и ограничений национального правового регулирования деятельности транснациональных проектов, организаций, юридических и физических лиц в киберинформационной сфере. Российская Федерация не подписала

Будапештскую Конвенцию[1] из-за противоречий в области понимания границ и возможностей правового регулирования информационных отношений (в контексте глобализации), а именно трансграничного доступа, хранения информации. В 2012 году был представлен проект конвенции в России, направленный на правовое регулирование транснациональных информационных отношений. Американский законодатель указал на недопустимость легитимизации цензуры в контексте нарушения политических и гражданских прав человека[2]. Законодатель в Российской Федерации разделяет данное положение, поскольку конвенция не отменяет Международный пакт о гражданских и политических правах, действующий независимо от нее.

Таким образом, получается, что провайдеры на абсолютно законных основаниях могут хранить вредную киберинформацию или заблокировать экономический сервер в IOT.

Все участники транснациональных информационных отношений понимают важность дальнейшего совершенствования и уточнения правового регулирования киберсреды. Проблемы информационных отношений исходят из неравномерности создания ИТ-технологий, цифровых феноменов и отсутствия единой системы правил регулирования. Интероперабельность инициирует сложную систему интеграции ИТ, подразумевая наличие открытой технологической сертифицированной инфраструктуры, обеспечивающей семантическую интероперабельность.

В качестве возможной рекомендации в учебном пособии с целью упорядочения и гармонизации процессов нормотворчества и правоприменения, в частности правового регулирования информационных отношений в киберсреде (в контексте глобализации), предлагается введение принципа интероперабельности в ст. 3 (Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации) федерального закона «Об информации, информационных технологиях и о защите информации».

---

[1] European Convention for the Protection of Human Rights and Fundamental Freedoms. URL: https://en.wikisource.org/wiki/European_Convention_for_the_Protection_of_Human_Rights_and_Fundamental_Freedoms (дата обращения: 04.01.2020).

[2] Савенков А. Н. Указ. соч. С. 5.

Совершенствование уровня технологической открытости информационной многофункциональной инфраструктуры в глобальном пространстве киберсреды будет способствовать более эффективному преодолению противоречий, возникающих в сфере гражданско-правовых отношений. В то же время необходимо подчеркнуть, что уровень технической, особенно семантической интероперабельности у разных стран не равномерен и не равнозначен.

Для снижения рисков сетецентрической деструктивной деятельности в киберсреде, руководствуясь принципом интероперабельности, важно своевременно выработать юридическую стратегию в виде нормативно-правовых актов, направленных на разработку стандартов обеспечения информационной безопасности в отношении ключевых интерфейсов информационной инфраструктуры.

Вопросы и задания для самостоятельной работы

1. Охарактеризуйте правовые подходы отечественных ученых, лежащие в основе правового регулирования киберсреды.

2. Чем обусловлен выбор принципов, лежащих в основе интероперабельности?

3. Представьте план работы с провайдером при организации информационной безопасности в образовательном учреждении.

4. Свидетелями каких событий, произошедших в январе 2022 года в Казахстане, стал весь мир?

5. Предусматривает ли сегодня федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» достаточное количество правовых инструментов для упорядочивания процедуры правового регулирования информационных отношений в киберсреде, блокировки деструктивного контента?

6. Охарактеризуйте дефиницию «вредная киберинформация».

7. Приведите наиболее удачные международные примеры правового регулирования противодействия вредной киберинформации.

3.2. Движения криминальной направленности в киберсреде

АУЕ как субкультура современной российской молодёжи*

На территории Российской Федерации наиболее распространена криминальная молодёжная субкультура (объединение), известная под аббревиатурой АУЕ*.

«Арестантское уголовное единство»* (АУЕ*, «Арестантско-уркаганское единство»*, «Арестантский уклад един»*) – деструктивная молодежная субкультура, пропагандирующая преступный образ жизни и навязывающая законы и порядки, принятые среди представителей криминального мира, находящихся в местах лишения свободы; некая идеология, которой придерживается определенная часть социальной среды, априори противостоящая официальной, государственной культуре и идеологии.

Носителями криминальной субкультуры являются преступные группировки и уголовники-рецидивисты, которые аккумулируют и передают преступный опыт подрастающему поколению.

АУЕ* базируется на дефектах правосознания, присущих подросткам и молодежи: правовой неосведомленности и дезинформированности, социально-правовом инфантилизме, социально-правовом негативизме. В результате их воздействия в молодежной криминальной среде складывается особое групповое правосознание со своими «законами» и нормами, которые выступают определяющим элементом субкультуры.

Подростки охотно воспринимают внешне привлекательные броские извращенные вкусы (приоритеты), сложившиеся в криминальной среде. Эти, как правило, циничные предпочтения проявляются как в досуговой культуре, так и в способах совершения преступлений, во взаимоотношениях с криминалитетом, выборе привилегий для «элиты», татуировках, кличках, внешнем оформлении правил, «законов» и традиций уголовного мира.

Важная роль при вовлечении молодежи в криминальную субкультуру отводится мифам, в которых прославляются образы «удачливого вора», «смелого разбойника», «несгибаемого парня», состав-

* Признана экстремистской организацией и запрещена на территории Российской Федерации.

ляющие основу и культивирующие «воровскую романтику», идею «воровского братства», «воровскую честность» и т. п.

При этом одна из ключевых особенностей АУЕ* – факт нарушения самими же сторонниками криминальных законов, или так называемых понятий, которых они якобы придерживаются.

Степень сформированности криминальной субкультуры, ее влияние на личность и группу бывают разными: в виде отдельных, не связанных друг с другом элементов; формирований (группировок криминальной направленности); наконец, она способна доминировать в конкретном учебном заведении (микрорайоне, населенном пункте), полностью подчиняя своему влиянию как маргинальную, так и законопослушную молодежь.

Главная задача создания ячеек АУЕ* – сбор средств в «фонд взаимопомощи» представителям преступного мира, находящимся в местах лишения свободы, так называемый «общак» («грев зон»). Он организован преимущественно в учреждениях среднего образования, где члены криминального движения собирают у детей деньги под предлогом того, что каждый из них может потом оказаться в местах лишения свободы и где им якобы также будут помогать. В действительности же средства попадают либо к «авторитетам», курирующим молодёжь через так называемых смотрящих, либо к людям, далеким от криминального мира.

Таким образом, можно определить цели распространения АУЕ*, преследуемые модераторами групп соответствующей тематики в соцсетях и лидерами существующих молодежных преступных формирований, к которым относятся:

– сбор средств в «фонд взаимопомощи» представителям преступного мира, находящимся в местах лишения свободы («общак»);

– получение выгоды путём рекламы и продажи товаров, произведённых в местах лишения свободы, что зачастую не соответствует действительности;

– вовлечение детей и молодёжи в совершение противоправных действий (в том числе в организацию насильственных и протестных акций в целях продвижения личных идей и интересов).

---

* Признана экстремистской организацией и запрещена на территории Российской Федерации.

Пропаганда антиобщественного поведения ведется преимущественно через социальные сети, кардинальным образом меняя идеологию несовершеннолетних, формируя у них искажённые, антиобщественные ценности.

Соцсети предоставляют возможность быстро найти единомышленников для общения по интересам. Если раньше молодежные преступные группы вели войны за расширение территориальных зон своего преступного влияния, то информационный век дает новые возможности мирового вовлечения.

В своей попытке стать частью преступного мира не понимающая реальных принципов его функционирования и управляемая столь же непосвященными лидерами АУЕ*, преследующими свои корыстные цели, молодёжь, преступив закон, оказывается «между двух огней»: с одной стороны, она уже перестает быть частью нормального, законопослушного общества и теряет шансы на светлое будущее, с другой – она так и не становится частью криминального мира, не может претендовать на блестящую «криминальную карьеру».

В этой связи особую значимость приобретает предупредительно-профилактическая работа в рассматриваемой социальной среде. Для ее эффективного проведения необходимо знать и правильно оценивать перечисленные аспекты функций, содержания, атрибутики криминальной субкультуры. Эти знания дают возможность успешно противостоять ее проникновению в подростковую среду и на самой ранней стадии развенчать ее «преимущества» по отношению к правовым и морально-нравственным нормам общества.

Признаки распространения криминальных субкультур

В целях противодействия распространению субкультуры АУЕ* необходимы своевременные выявление и профилактика преступного образа мыслей и поведения в среде обучающихся. В этой связи нужно в первую очередь обратить внимание на поисковые признаки применительно к вовлечению молодежи в АУЕ*. Среди них выделяются две группы: косвенные и прямые.

* Признана экстремистской организацией и запрещена на территории Российской Федерации.

В группу косвенных признаков вовлечения несовершеннолетних в АУЕ* входят:

– активное изучение детьми и подростками материалов, содержащих идеологию АУЕ*, в том числе в сети Интернет;

– частое и необоснованное появление в молодежных тусовках и коллективах учащихся лиц, освободившихся из мест лишения свободы, в том числе находящихся под надзором полиции;

– использование для общения и распространения материалов конспиративных способов связи – незарегистрированных («левых») симкарт, мессенджеров, закрытых групп в соцсетях, анонимайзеров и др.

К прямым относятся признаки, непосредственно указывающие на вовлечение несовершеннолетних в АУЕ* со стороны организованных преступных групп и преступных сообществ либо так называемых положенцев – «смотрящих», назначенных контролировать район или образовательное учреждение, а именно:

– популяризация отдельными лицами воровского образа жизни, почитание авторитетов преступного мира («воров в законе»), изучение их биографий, трансляция информации о них;

– повышенный интерес со стороны криминальных группировок и их членов к группам подростков и молодежи образовательных организаций с признаками асоциального поведения;

– попытки представителей криминалитета установить связи с отдельными группами молодежи;

– изготовление и распространение конкретными лицами, в том числе посредством Интернета и СМИ, материалов, пропагандирующих АУЕ*, а также призывов присоединяться к субкультуре;

– наличие в группе подростков строгой иерархии по аналогии с тюремной;

– частичное соблюдение членами группы неписаных правил и норм преступного мира, обязательных для «воров в законе» и осужденных, заключённых и лиц, относящихся к криминальным сообществам («понятия», «воровской закон», «тюремный закон»);

– нанесение подростком на тело татуировок, распространение изображений, аббревиатур и лозунгов (нанесение на предметы, стены

* Признана экстремистской организацией и запрещена на территории Российской Федерации.

жилых домов, помещений), характерных для лиц, отбывающих (отбывших) сроки лишения свободы;

– вовлечение детей и подростков, не достигших совершеннолетия, в совершение преступлений и правонарушений, в том числе связанных с нарушением общественного порядка: массовых беспорядков, актов вандализма, нападений на сотрудников правоохранительных органов, хулиганских действий.

Один из важнейших индикаторов распространения АУЕ* – появление символики и аббревиатур движения на зданиях, сооружениях, особенно в образовательных организациях, а также бумажных носителей информации, пропагандирующих АУЕ* с использованием рисунков и лозунгов (чаще их аббревиатур), расшифровка которых зачастую содержит нецензурную лексику (АУЕ*, ЛХВС*, СЛОН*, БАРС*, ЖВСС*, АВОЕ*, ТУЗ*, КОТ*, БОГ*, ВЕК*, ВОЛК*).

Рекомендации по неотложным действиям при выявлении признаков криминальной субкультуры

Эффективность профилактики распространения криминальной субкультуры среди несовершеннолетних зависит от таких обязательных условий, как своевременность, законность, дифференцированность, правильная последовательность, комплексность и др.

Ключевыми мерами по профилактике распространения криминальной субкультуры выступают:

– активное вовлечение детей в культурную и общественную жизнь (например, конкурсы студенческих и школьных команд по многоборью, владению профессией и т. д.);

– обеспечение доступности дополнительных образовательных программ, создание условий в учебных учреждениях для работы творческих объединений по интересам для несовершеннолетних;

– выявление и точечная работа с подростками, находящимися в социально опасном положении, не посещающими или систематически пропускающими по неуважительным причинам занятия в школе или сузе;

* Признана экстремистской организацией и запрещена на территории Российской Федерации.

– выявление семей, находящихся в социально опасном положении, и оказание им помощи в обучении и воспитании детей.

В случае выявления признаков распространения криминальной субкультуры в образовательной организации необходимо:

1) оперативно обратиться в подразделение по делам несовершеннолетних органов внутренних дел (далее – ПДН);

2) провести совместно с сотрудниками ПДН анализ масштаба распространения криминальной субкультуры в рамках образовательной организации;

3) сформировать план мероприятий по противодействию распространению криминальной субкультуры с учетом специфики конкретной образовательной организации;

4) организовать поиск и отбор признанных авторитетных организаций (государственных и общественных), способных вести работу с молодежью по выводу ее из криминальной среды и привлечь к ней молодежных лидеров, историков, психологов.

При возникновении в образовательном учреждении чрезвычайных ситуаций, связанных с противоправными действиями активных сторонников криминальной субкультуры, рекомендуется:

1) незамедлительно обратиться в местные органы полиции, Росгвардии, МЧС для пресечения чрезвычайной ситуации и минимизации ее последствий;

2) при возможности – организовать эвакуацию пострадавших и не вовлеченных в противоправные действия лиц из учреждения;

3) при блокировании инициаторами хулиганских действий выходов из учреждения – изолировать преподавательский состав и обучающихся в отдельных помещениях, закрыв двери и создав искусственные препятствия.

При получении информации о распространении субкультуры вне образовательных учреждений следует совместно с правоохранительными органами:

1) определить возможные «места притяжения» молодежи (спортивные площадки, стадионы, парковые зоны, торгово-развлекательные центры), а также конкретные точки и время сбора лиц (подростков и молодежи) из числа приверженцев криминальной субкультуре;

2) выявить лидеров и активных участников криминального движения («положенцев», «смотрящих» по району), вовлекающих детей и молодежь в деятельность АУЕ*, в том числе через Интернет и массовую культуру. При отсутствии угрозы жизни и здоровью зафиксировать их на фото;

3) в целях проверки информации и принятия мер профилактического характера информировать о выявленных фактах правоохранительные органы, оказать им содействие в опознании возможных лидеров группировок.

В случае выявления распространения криминальной субкультуры в Интернете:

1) попытаться самостоятельно определить администраторов, модераторов, редакторов группы/паблика/страницы, популяризирующих криминальную субкультуру АУЕ*, не вступая в общение с ними;

2) подготовить обращение в адрес администрации социальной сети через соответствующую форму с указанием адреса страницы, популяризирующей криминальную субкультуру АУЕ*, данных администраторов, модераторов, редакторов группы/паблика/страницы, а также ссылок на посты (материалы), непосредственно содержащие деструктивный контент и популяризирующие криминальную субкультуру АУЕ*;

3) подготовить обращение в адрес органов Прокуратуры России и Роскомнадзора с указанием адреса страницы в сети Интернет, популяризирующей криминальную субкультуру АУЕ*, а также ссылок на посты (материалы), указанные выше, с просьбой проведения проверки и блокировки.

По мнению большинства специалистов, наиболее эффективная мера по профилактике распространения субкультуры – публичное развенчивание мифа о романтичности воровского мира, демонстрация его объективной несправедливости и жестокости, а также информирование целевой аудитории, в том числе в профилактических целях, об истинном положении осужденных в тюрьмах, проблемах их социальной адаптации и реабилитации.

---

* Признана экстремистской организацией и запрещена на территории Российской Федерации.

Вопросы и задания для самостоятельной работы

1. Раскройте сущность сетевых движений радикальной направленности и деструктивных субкультур терминальной направленности.
2. Укажите основные движения криминальной направленности, действующие на территории Российской Федерации.
3. Назовите цель движения криминальной направленности «Арестантское уголовное единство» (АУЕ*).
4. Охарактеризуйте особенности идеологии движения криминальной направленности АУЕ*.
5. Дайте общую характеристику контенту движения криминальной направленности АУЕ*, размещенному в сети Интернет.
6. Назовите особенности организации движения криминальной направленности АУЕ* в сети Интернет в доступных для мониторинга на территории Российской Федерации социальных сетях.

3.3. Субкультуры аутодеструктивной направленности в киберсреде

Мониторинг и анализ информации о распространении в сети Интернет групп суицидальной направленности (так называемых групп смерти) позволили также причислить их к результатам воздействия на молодежь субкультурных образований.

«Группы смерти» представляют собой форму организации подросткового субкультурного течения, основная идея которого – пропаганда идей суицида и причинения вреда самому себе.

Продвижение суицидальной тематики не только оказывает пагубное воздействие на несформировавшуюся психику подростков и стимулирует их к совершению самоубийств, но ведет к росту социальной напряженности, формированию атмосферы страха в обществе, росту недоверия к органам государственной власти.

В качестве подтверждения результатов деструктивного влияния указанных ресурсов интернет-сообществ специалисты в области информационной безопасности приводят весьма плачевную статистику: в 2015 – 2017 годы зафиксировано более 200 случаев суицида среди подростков в возрасте 11 – 17 лет.

---

* Признана экстремистской организацией и запрещена на территории Российской Федерации.

Деструктивная идеология распространяется посредством тематических интернет-сообществ в социальных сетях: «ВКонтакте» (#«f57», #«f58», #«тихий дом», #«рина», #«няпока», #«киты», #«море китов» и др.) – общее количество участников более 200 тыс. чел., Одноклассники – 30 тыс. чел., видеохостинг Youtube* – 160 тыс. чел., Facebook* – 30 тыс. чел., Instagram* – 139 тыс. чел., Twitter* – 10 тыс. чел.

Аналитики, привлеченные к исследованию современного феномена подростковых самоубийств, среди активных факторов, ведущих к суициду, называют деятельность администраторов пабликов соответствующей тематики в соцсетях, использующих в своей работе психоманипулятивные технологии воздействия на личное и групповое сознание. В этой связи при рассмотрении содержания деятельности администраторов «групп смерти» следует в первую очередь обратить внимание на указанные особенности и механизмы влияния на подростка.

По заключению психиатров и психологов, применяемые модераторами «групп смерти» психотехники сходны с теми, что используют деструктивные неокульты и исламские радикальные формирования.

Как правило, группы с соответствующей тематикой обладают рядом признаков (также характерных и для деструктивных психокультов и сект), по которым их можно выделить из остальных популярных интернет-сообществ деструктивной направленности, нацеленных на увеличение количества подписчиков, а не на совершение ими определенных действий:

1. В «группах смерти» формируется так называемый культ личности администратора, являющегося непререкаемым авторитетом для других членов сообщества, полностью ему преданных. Он служит источником новой информации, преподносимой в суггестивном ключе и требующей безусловного принятия и полного подчинения (выполнение «заданий» в игре).

2. Характерной чертой считается применение администраторами «групп смерти» манипулятивных методик убеждения и контроля, направленных на «реформирование мышления».

3. Администраторы активно используют специальные способы повышения внушаемости: прерывистый сон (понуждение к ночным

* Запрещены для использования на территории Российской Федерации.

конференциям), что вызывает сонливость, утомление, неустойчивость настроения, нарушение сна; стимуляцию ощущения безвыходности положения, физического истощения (отказ от еды), употребления алкоголя либо кофе и энергетиков, что способствует эмоциональному возбуждению; создание дефицита времени для принятия решения.

При вовлечении в Интернете в аутодеструктивные группы происходит корректировка информационного потока «жертвы», выражающаяся в побуждении к присоединению к группам, содержащим шоковый, деструктивный контент. Информация сообщества для обсуждения и оценки подается и регулируется администратором, дозируется (сообщается только часть сведений, в результате чего картина реальности искажается в нужную сторону). Смешивание истинных фактов со всевозможными предположениями, допущениями, гипотезами, слухами (так называемый ядовитый сендвич) приводит к когнитивным сдвигам восприятия и самовосприятия.

Преступник, который вовлекает молодежь в аутодеструктивную группу, старается сделать так, чтобы его деятельность влияла на:

1. Стимулирование у «жертвы» зависимости от группы, страха перед выходом из нее.

2. Контроль среды, включающий контроль общения с внешним и внутренним миром (так называемый внутренний диалог), что приводит к потере личной свободы и слиянию с контролирующей его группой до такой степени, что проникшие в его сознание групповые представления постепенно начинают управлять его внутренним диалогом.

3. Мистическое манипулирование – стимуляция поведения, запрограммированного группой и идеологическим руководителем. Член группы не понимает, что определенный тип поведения и чувств (новая мировоззренческая концепция) не появились спонтанно (мистически), а были внешне индуцированы, но начинает осознавать себя участником авангарда для достижения какой-то «высокой цели». Для этого администратор мистифицирует специальные манипулирующие инструменты (квесты, задания, символика и собственная личность).

4. Рост невыполнимых стандартов поведения, способствующих созданию атмосферы вины перед окружающими и стыда.

Независимо от того, какие усилия прикладывает человек, он всегда терпит неудачу. В случае с «группами смерти» это задания,

вызывающие когнитивный диссонанс, чувство неловкости, стыда и, как следствие, внушаемость. Например, у ребенка, любящего родителей, требуют детально обдумать и описать способ их убийства. В других случаях требуют прислать фото в обнаженном виде и пр. Администратор выступает в роли судьи, используя страх, вину и стыд как эмоциональные рычаги для контролирующего и манипулирующего влияния.

Непременное условие нахождения в «группе смерти» – культ личной исповеди, ведущий к разрушению границ личности. Это своего рода предписание делиться и признаваться в любой мысли, чувстве или действии, которые можно заподозрить в несоответствии групповым правилам.

Акцентируется внимание на «несправедливости» общества, жизни, бесперспективности, одиночестве вне группы, стимулируется желание «отомстить» своей смертью.

Как правило, мысль о суициде доводится до целевой аудитории двумя способами:

1. Прямые внушения – «прыгай», «сделай», «выполни» задания в игре и прочие прямые указания и предписания администратора группы (например, как вести себя в той или иной ситуации).

2. Косвенные внушения: последовательность принятия решений (внутреннее «да» на слова оператора несколько раз), подразумеваемое указание (когда счетчик закончится – произойдет нечто важное), встроенные в текст внушения, а также рассказы и обсуждения суицидов и смертей других людей, специально подобранный шок-контент – суицидальный контент (в том числе креолизованные тексты, эпиграфы и цитаты значимых людей, посвященные суицидальной тематике, и многое другое).

Этапы механизма склонения подростка к суициду:

1. Возбуждение любопытства к тематике с использованием специфического «запретного» контента.

2. Сбор информации о подписчиках, их родных, близких, окружении. Начало индивидуальной психологической обработки с использованием перечисленных методик для выбора конкретных «жертв».

3. Выслушивание проблем подростка (зачастую групповое), т. е. так необходимое внимание к его персоне в непростой возрастной период.

4. Появление «проводника», «психолога», который демонстрирует «правильное направление», указывает путь к «истине», «счастью», зачастую даже «отговаривает» от суицида в целях формирования доверительной, устойчивой связи.

5. Приглашение в «круг избранных», где есть возможность познания истины, изменения себя, получения представления о своем месте в мире. Цель – отбор «игроков в смерть».

6. Начало «игры»: интеграция в группу, перечень усложняющихся заданий, появление новых персонажей, «работающих» с игроком (как правило, более высокого уровня, нежели «вовлекатели» и «отсеиватели»), которые снижают критичность восприятия у играющих, реформируют мышление, меняя систему ценностей.

7. Продолжение «игры». Здесь используется массированное воздействие на сознание подростка, направленное на усугубление имеющихся или созданных проблем для подготовки к осуществлению желаемого поведения.

8. Кризис в «игре». Методы: углубление психологических проблем до степени «непереносимости» (адресная работа, вплоть до угроз и шантажа); разъяснение методов достижения «пути к истине»; предложение желаемого поведения как безальтернативного выхода из ситуации; «активизация» поведения через задания, непосредственно связанные с самоубийством (выбор места, музыкального сопровождения, последних слов, таймера с обратным отсчетом); изучение и применение дыхательных и трансовых техник.

9. Завершение «игры». Активизация «триггера».

В настоящее время вновь прослеживается тенденция к росту популярности «групп смерти» в связи с широтой охвата детей и подростков, пользующихся социальными сетями.

Отмечается появление феноменов аналогичных псевдогрупп, создаваемых администраторами, желающими получить популярность (раскрутить паблики в сети), или новых «групп смерти» под прикрытием пабликов, где бесплатно оказывается поддержка пострадавшим.

Вести работу с подростками, находящимися под воздействием «групп смерти», необходимо крайне аккуратно, так как они находятся

под влиянием группы даже после формального выхода из нее. Поэтому они крайне отрицательно воспринимают внешние попытки выяснения обстоятельств, связанных с игрой и кругом лиц, которые «работали» с ними, используют рекомендуемые администраторами методы «отказа» и разговорные клише.

Рекомендации по выявлению суицидальных наклонностей и предотвращению самоубийств среди подростков и молодежи

Для выявления суицидальных наклонностей рекомендуется проводить среди референтных групп различные исследования в форме тестирований (анонимные и персонифицированные), индивидуальных консультаций, бесед и пр. Основная цель подобных исследований – определение принадлежности объекта к «группе риска» по суициду.

Ключевыми признаками, требующими особого внимания, являются:

1. Нарушение межличностных отношений:

– наличие проблем в семье, смерть близких, уход из семьи или развод родителей и др.;

– искусственное ограничение круга общения подростка, влекущее выделение в коллективе одиночек, изгоев;

– конфликты со сверстниками, педагогами, близкими людьми; наличие психологических факторов, оказывающих давление на подростка;

– постоянное физическое и (или) психическое насилие.

2. Наличие эмоциональных нарушений.

3. О планируемом самоубийстве говорит приведение своих дел в порядок.

4. Прощание – выражение благодарности различным людям за помощь в разные периоды жизни.

5. Оставление письменных обращений, указаний (в письмах, записках, дневнике), запись видеообращений, вербальные указания на планируемый суицид.

Для профилактики совершения суицидов необходимо уделять внимание развитию антисуицидальных факторов личности – это усиление положительных жизненных установок, жизненной позиции, а также акцентирование внимания личности на душевных переживани-

ях, препятствующих осуществлению суицидальных намерений. К ним относятся:

– эмоциональная привязанность к значимым родным и близким людям, степень значимости отношений с ними;

– выраженное чувство долга, обязательность;

– концентрация внимания на состоянии собственного здоровья, ценности собственного тела, боязни причинения себе физического ущерба;

– усиление необходимости учета общественного мнения и избегания осуждения со стороны окружающих, представления о позорности самоубийства и неприятии (осуждении) суицидальных моделей поведения, негативная проекция своего внешнего вида после самоубийства;

– стимулирование убеждения о неиспользованных жизненных возможностях, появления жизненных, творческих, семейных и других планов, замыслов;

– развитие в подростке духовных, нравственных и эстетических критериев в мышлении, психологической гибкости и адаптированности, умения компенсировать негативные личные переживания, использовать методы снятия психического напряжения.

Чем больше жизнеутверждающих свойств у человека, чем сильнее его «психологическая защита» и внутренняя уверенность в себе, тем прочнее его антисуицидальный барьер.

В этой связи родителям, педагогам и психологам необходимо уделять внимание профилактике депрессий у подростка. Для этого нужно обсуждать с ребенком его проблемы, строить планы на будущее, помогать ему соблюдать режим дня и изменить образ жизни, заняться новыми делами.

Вопросы и задания для самостоятельной работы

1. Дайте понятие движений, продвигающих аутодеструктивное поведение.

2. Укажите цели движений, продвигающих аутодеструктивное поведение.

3. Раскройте идеологию движений, продвигающих аутодеструктивное поведение.

4. Охарактеризуйте контент движений, продвигающих аутодеструктивное поведение, размещенный в сети Интернет.

5. Назовите особенности организации движений, продвигающих аутодеструктивное поведение, информационно-пропагандистской работы в сети Интернет в доступных для мониторинга на территории Российской Федерации социальных сетях.

3.4. «Скулшутинг»* («колумбайн»*) в киберсреде

Одна из крайних форм проявления деструктивного поведения среди подростков из числа учащихся образовательных учреждений – радикальное субкультурное течение «скулшутинг»* (стрельба в школе).

«Скулшутинг»* следует трактовать как любую форму немотивированных насильственных действий в образовательных учреждениях, совершаемых учащимся (группой учащихся) в отношении преподавателей и учеников с использованием оружия и подручных средств.

Первым примером «скулшутинга»* стали трагические события в американской школе «Колумбайн» (округ Джефферсон, штат Колорадо, США) в апреле 1999 года. Учащиеся старших классов Эрик Харрис и Дилан Клиболд совершили нападение на учеников и персонал школы с применением стрелкового оружия и самодельных взрывных устройств. В результате были убиты 13 человек (12 учеников и учитель) и ранены 23 человека. Оба преступника покончили жизнь самоубийством, застрелившись.

Массовое убийство в октябре 2018 года в политехническом колледже в г. Керчи по количеству жертв стало самым крупным – 21 человек убит, 67 пострадали. Сам убийца в сообществах «скулшутинга»* не состоял, но сценарий совершенного им преступления практически повторил события, произошедшие в школе «Колумбайн». Для участников террористического движения он стал примером для подражания.

Как и в случае с другими деструктивными субкультурами, «скулшутинг»* стал столь популярен благодаря распространению в сети Интернет (преимущественно в соцсетях).

---

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

В последнее время органами власти приняты беспрецедентные меры по «зачистке» соответствующих групп в соцсетях, однако в зарубежном сетевом сегменте «скулшутинговые» паблики по-прежнему активно множатся.

Администраторами тематических групп в социальных сетях являются наиболее активные последователи субкультурного течения. В большинстве случаев это несовершеннолетние, которым фактические создатели и модераторы тематических ресурсов после их развития передают права администрирования. Таким образом они обеспечивают себе дополнительные меры конспирации и продолжают создавать новые страницы и чаты в Интернете.

Как правило, для сообществ подобного рода характерно наличие таких признаков, как «мода на оружие»; романтизация и оправдание действий «скулшутеров»; пропаганда насилия над преподавателями и учащимися с использованием дискредитирующих видео, демотиваторов и челленджей; видеозаписи сцен насилия и убийств (в первую очередь массовых расстрелов). Среди факторов, способствующих вовлечению подростков в «скулшутинг»* и провоцирующих их к нападению на сверстников, специалисты выделяют:

– проблемы в семье, отсутствие внимания к проблемам ребенка со стороны родителей, ссоры с членами семьи, физическое и психическое насилие;

– длящиеся конфликтные ситуации со сверстниками и педагогами, к которым относится буллинг (травля) учащегося – агрессивное преследование одного из членов коллектива (особенно актуально для образовательных учреждений) со стороны других;

– наличие у подростка доступа к огнестрельному оружию (охотничьему, травматическому, пневматическому), химикатам, горючим смесям;

– индивидуальные психологические особенности (повышенная внушаемость и ведо́мость) или психические отклонения.

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

К признакам, характеризующим подростка в качестве приверженца террористического движения «скулшутинг»*, относятся:

– подражание «скулшутерам» в стиле и одежде: соответствующая причёска, цвет волос, предметы одежды (длинный черный плащ, высокие ботинки, стиль «милитари», футболки с надписями «Natural Selection», «Естественный отбор», «Wrath», «Гнев», «Ненависть»);

– замкнутость, стремление отгородиться от реального мира, погрузиться в свои переживания и фантазии, преувеличенная эмоциональная реакция, систематическое нарушение дисциплины и прогулы;

– наличие глубоких познаний о «скулшутинге»*, насилии, личности убийц (Эрик Харрис, Дилан Клиболд, Дилан Руф, Владислав Росляков, Митчелл Джонс, Эндрю Голден, Джефри Уиз и др.);

– сбор и накопление материалов с соответствующим «шок-контентом» (видеозаписи убийств, самоубийств, происшествий, актов терроризма, пыток), наличие большого количества аудиозаписей, характерных для «скулшутеров» (например, отдельные музыкальные композиции групп Foster The People – Pumped up Kicks, Rammstein, KMFDM и др.);

– высказывание косвенных или прямых угроз в адрес будущих жертв, использование в сетевом и речевом общении характерных слов и словосочетаний;

– ведение дневника с именами других людей без указания цели, изображениями жутких, пугающих картин, заштрихованными чернилами листами.

Также психологи выделяют следующие особенности «скулшутеров», характерные для общения в соцсетях: участие в тематических сообществах (группах, событиях, беседах) в социальных сетях и мессенджерах, связанных с оружием, тактикой ведения боя и выживанием в экстремальных условиях; мониторинг пабликов, содержащих описание методов убийства, изготовления оружия, самодельных взрывных устройств (СВУ), зажигательных смесей; создание псевдо-

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

нима с личными данными убийц и «скулшутеров»; наличие в «друзьях» лиц, также увлекающихся деструктивным контентом.

Для своевременного выявления и предупреждения акций «скулшутинга»* необходимо ориентироваться в признаках их подготовки и совершения акции:

– внешние признаки: одежда (длиннополый плащ, удобная обувь, футболка с характерными надписями и изображениями, перчатки); наличие больших, тяжелых сумок и рюкзаков;

– психосоматические признаки: бледность кожных покровов, расширенные зрачки, «пустой» взгляд, тремор конечностей, непроизвольное повторение характерных фраз (молитв), ощупывание под одеждой оружия и самодельных взрывных устройств, отвлеченный немигающий взгляд; избавление потенциальным «скулшутером» от «лишнего»: обнуление денежных счетов, продажа личного имущества (техники, гаджетов, одежды), уничтожение (часто путем сжигания) бумажных и электронных носителей информации;

– публикация в Интернете сообщений с датой, ключевой фразой или другим неочевидным намеком на будущее событие с использованием характерных словосочетаний, изображений;

– подготовка к ведению онлайн-трансляции акции, привлечение внимания аудитории тематических групп в соцсетях;

– оставление предсмертных записок и видеообращений.

*Рекомендации по профилактике акций «скулшутинга»**

1. Контроль руководством учебных заведений и правоохранительными органами соблюдения персоналом общих требований безопасности на объектах образования. Обеспечение недопустимости проноса в образовательное учреждение любых видов оружия, колющих и режущих предметов, взрывоопасных веществ, зажигательных смесей, СВУ, их компонентов, устройств блокирования выходов из здания.

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

2. Проведение специальных занятий по безопасности с учителями и сотрудниками охраны учреждения в целях повышения уровня знаний о соответствующих признаках в поведении учащихся с привлечением специалистов правоохранительных органов.

3. Активное применение профилактических мер по борьбе с травлей учащихся. При обнаружении признаков соответствующей проблемы не решать ее публично – необходимо определить и провести индивидуальные беседы с жертвой и «агрессорами». С участием психолога помочь жертве в адаптации к коллективу.

При обнаружении у учащегося признаков готовности к «скулшутингу»* следует:

1. Информировать руководство образовательного учреждения и правоохранительные органы.

2. В случае высокой готовности подростка к совершению акции «скулшутинга»* следует исключить проведение с ним профилактических бесед администрацией школы и родителями, не допускать к учащемуся специалистов, не имеющих психологического образования и опыта/знаний в соответствующей сфере.

3. Важно изолировать потенциального «скулшутера» от других учащихся, затем привлечь специалистов (психологов, сотрудников полиции, органов безопасности, медицинских работников).

Результаты анализа популярных интернет-ресурсов (соцсетей и видеохостингов) доказывают, что среди подростков тематика «скулшутинга»* продолжает пользоваться популярностью.

С учетом повышенного внимания молодежной аудитории к тематике «скулшутинга»* специалисты прогнозируют возможное совершение приверженцами террористического движения массовых расстрелов в учебных заведениях; убийства одноклассников единичного, а не массового или серийного характера; нападения на учителей с холодным оружием; блокирование выходов из учебных заведений с последующим поджогом или подрывом СВУ; захват группой подростков заложников.

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

Вопросы и задания для самостоятельной работы

1. Дайте понятие сетевому молодежному движению террористической направленности «скулшутинг»* («колумбайн»*).

2. Укажите цели сетевого молодежного движения террористической направленности «скулшутинг»* («колумбайн»*).

3. Раскройте идеологию сетевого молодежного движения террористической направленности «скулшутинг»* («колумбайн»*).

4. Охарактеризуйте контент сетевого молодежного движения террористической направленности «скулшутинг»* («колумбайн»*), размещенный в сети Интернет.

5. Назовите особенности организации сетевым молодежным движением террористической направленности «скулшутинг»* («колумбайн»*) информационно-пропагандистской работы в сети Интернет в доступных для мониторинга на территории Российской Федерации социальных сетях.

3.5. Деятельность М.К.У.* («Маньяки Культ Убийств»*) в киберсреде

М.К.У.* – террористическая молодежная организация, главная цель которой – популяризация убийств и насилия, а также склонение к данным действиям участников сообществ соответствующей тематики в сети Интернет.

Популяризация М.К.У.* – еще одно массовое криминальное явление в современных социальных сетях. Как и аутодеструктивные группы, данная информационная угроза связана с десакрализацией смерти.

Появившееся в 2017 году на Украине сообщество под названием «Маньяки Культ Убийств»* (М.К.У.*) достаточно быстро приобрело популярность в молодежной среде нашей страны, прежде всего в интернет-пространстве.

В начале своего становления в 2017 году М.К.У.* представляло собой небольшое фан-сообщество, целью которого было привлечь к себе максимальное внимание и выбиться в тренды медиапространства

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

посредством использования запретных тем, касающихся жестокости, насилия.

Создателем и главным координатором ячеек М.К.У.* является украинский неонацист Егор Краснов, житель г. Днепра (полные установочные данные отсутствуют). В подростковом возрасте Краснов вступил в молодёжную ультраправую организацию, где нашел единомышленников. Когда его исключили из организации за чрезмерный радикализм, он вместе с соратниками создал «М.К.У.*Чат» и возглавил экстремистскую деятельность днепровской ячейки. На ее счету – убийства, избиения, покушения на убийства лиц неславянской внешности и зависимых от ПАВ лиц. В декабре 2020 года Краснов был задержан украинскими правоохранительными органами в качестве подозреваемого.

В период с 2020 по 2021 год на территории стран СНГ под воздействием идеологии М.К.У.* начали формироваться отдельные сообщества последователей движения в онлайн- и оффлайн-пространстве, целью которых среди прочего было занятие «трэш-контентовых» ниш в медиа-пространстве.

В последнее время между сообществами «скулшутинг»* и М.К.У.* прослеживается четкая связь. Так, с января 2022 года во всех ресурсах, посвященных колумбайн*-движению, активно рекламируются М.К.У.*-сообщества, в которых распространяется одинаковый контент, полностью копирующий или схожий с контентом групп, посвященных «скулшутингу»*.

С началом специальной военной операции во всех ресурсах, посвященных колумбайн*-движению, стали появляться рекламные записи М.К.У.*-сообществ с призывами к насилию и убийствам с целью организации терактов на территории России.

С 24 февраля 2022 года группы, посвященные М.К.У.*, стали рассылать сообщения и совершать звонки с заведомо ложной информацией о готовящихся террористических актах в общественных местах. Отчеты о такой деятельности выкладываются в закрытые Telegram-каналы, посвященные М.К.У.*

В марте 2022 года на Telegram-канале М.К.У.* «MIRROR 12» главный координатор деятельности М.К.У.*-сообществ совместно с

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

главным координатором действий современного колумбайн*-комьюнити на территории России и стран СНГ вел поиск лиц, владеющих навыками минирования и изготовления самодельных взрывных устройств, а также утверждал, что «боевые действия на Украине необходимо использовать для совершения террористических актов, убийств и дестабилизации обстановки в России».

В этой связи есть основания полагать, что координаторы деятельности М.К.У.* и движения «колумбайн»* действуют под контролем спецслужб Украины, а группировка «Маньяки Культ Убийств»* была создана ими для подготовки и совершения преступлений экстремистской и террористической направленности на территории России.

Стоит отметить тот факт, что в марте 2022 года администрация М.К.У.*-сообществ совместно с администраторским составом колумбайн*-сообществ России искала участников игр, проживающих в местах, где в рамках СВО проходят столкновения нашей страны и Украины, для «специального» задания.

И уже 5 апреля 2022 года был «репостнут» первый видеоотчет убийства человека из закрытого Telegram-канала «Н.С.Т.»* в канал, посвященный колумбайн*-движению и М.К.У.* «Killyou(All)».

В настоящее время главные координаторы действий М.К.У.*-ячеек дают разрешение на проведение насильственных акций, координируют даты проведения, выбор орудия преступления, инструктируют по изготовлению самодельных взрывных устройств и т. д. Большинство акций снимаются на видео, потом монтируются и размещаются в общих чатах.

В последнее время начали проявлять активность паблики, ранее рекламируемые в Telegram-сообществах, посвященных «колумбайну»*, но не транслирующие их идеи. Активность заключается в призывах к дестабилизации действующей власти на территории России.

Подводя итог вышесказанному, можно отметить связь современного колумбайн*-движения и М.К.У.*-комьюнити. Несмотря на то что М.К.У.*-сообщества изначально базировались исключительно на идеях неонационализма, М.К.У.* может объединять разных идеологически направленных участников на основе общей идеи убийства и

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

насилия, что значительно расширяет потенциальную аудиторию и облегчает распространение культа убийц.

Сущность М.К.У.* основывается на идеологии расового, национального или личностного превосходства над кем-либо, а также геноцида всех людей, не удовлетворяющих критериям человека, имеющего право на жизнь в рамках деструктивной ячейки «Маньяки Культ Убийств»*.

Как перспективный метод вовлечения молодежи в деятельность М.К.У.*-сообщества модераторы используют геймификацию, которая применяется большинством современных деструктивных сетевых движений.

Геймификация предполагает обязательное выполнение заданий «игры» для вступления в организацию и получения доступа к медиаресурсам более закрытых типов.

Также М.К.У.* проводит челленджи «дней очищения», ориентируя своих сподвижников на единовременное совершение убийств и терактов и нанося дату «дня очищения» в виде граффити на объекты городской инфраструктуры.

Как и любой субкультуре, террористической организации свойственна своя иерархия (по возрастанию значимости):

– потребитель контента – рядовой подписчик ресурса, посвященного идеям М.К.У.*, не вовлеченный в преступную деятельность;

– участник «игры» – подписчики закрытых Telegram-каналов, выполняющие задания закрепленных за ними кураторов «игр». Выполняемые ими задания имеют преимущественно противоправный характер (от членовредительства и порчи чужого имущества до реальных убийств животных и людей). Чем сложнее и аморальнее участник «игры» выполняет задание, тем большим авторитетом он пользуется как у кураторов «игр», так и у других ее участников;

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

– кураторы игры – лица, непосредственно передающие задания «игр» М.К.У.*, а также ответственные за оценку качества его выполнения и отбор лучших «отчетов игр»;

– администратор сообщества – главный администратор интернет-сообщества, размещающий отчетные видеоролики о результатах выполнения заданий «игр», а также согласующий эти задания с главным администратором сети сообществ и кураторами «игр».

Главный администратор сети сообществ – лицо, которое официально определяет направление деятельности ряда сообществ, посвященных М.К.У.*

В зависимости от классификации М.К.У.*-сообщества (открытое/закрытое/частное), осуществляющего противоправную деятельность, с обычным потребителем контента не связываются остальные звенья иерархии, однако для членства в некоторых закрытых сообществах от потребителя контента требуется использование средства идентификации участника (это могут быть характерные для М.К.У.* слова, символы, изображения на аватарке и т. д.), также потребитель контента может сам связаться напрямую с куратором «игры» с целью продвижения в иерархии до участника «игр». Участник «игры» закреплен за своим куратором, который выдает ему задания и оценивает их выполнение. Связь поддерживается с помощью сторонних анонимных мессенджеров по типу Jabber и element, иногда с помощью закрытых Telegram-чатов с функцией автоудаления сообщения через 15 секунд после отправки с целью максимальной анонимизации как участника «игры», так и его куратора. Для идентификации конкретного участника «игры» используются вымышленные имена и прозвища. Действия куратора «игры» координирует администрация сообщества, в рамках которого выкладываются отчетные материалы «игр», также эта администрация дает инструкции по техникам анонимного пребывания в сети Интернет. Как и в случае звена «участник “игры” – куратор», используются средства связи в сторонних средствах анонимной отправки сообщений. Финальным и главным звеном является обще-

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

принятый лидер разных групп сообществ, объединенных идеей М.К.У.*, который определяет вектор преступной деятельности культа убийц.

*Признаки, характерные для члена движения М.К.У.**

Пользователи, причисляющие себя к культу убийц, имеют ряд схожих признаков в своих интернет-аккаунтах:

1. Характерные аббревиатуры, символы, слова, числа в названиях, описаниях, адресах и аватарах страниц, несущие в себе следующий смысл:

а) даты каких-либо террористических акций и преступлений: «1999», «04.20», «04.20.1999» и т. д.;

б) факты из жизни известных преступников, их фамилии, имена и прозвища: «Vodka» (никнейм в компьютерной игре Дилана Киболда), «Брейвик», «Харрис», «Росляков», «Потрошитель» и т. д.;

в) экстремистские обозначения: «14/88», «o/» и т. д.;

г) экстремистские лозунги, призывы к насилию, цитаты из экстремистской литературы: «Да прольется кровь», «Национальный террор» и т. д.;

д) прямое указание к принадлежности М.К.У.*: «мку», «маньяк», «убийца», «tcc» и др.

2. Использование в качестве аватаров кадров террористических актов, изображений известных преступников/террористов, фотографий актеров, сыгравших того или иного преступника, оккультных символов (пентаграмма, изображение сатаны).

3. Размещение и распространение контента оккультного, сектантского, психоделического, порнографического, экстремистского характера.

4. Использование нестандартных символов («(«,»)», «?», «/» и т. д.) для составления символьного изображения оружия, экстремистских и оккультных символов, например: «η γ ζ ε η».

---

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

Помимо индикаторов вовлеченности человека в культ убийц в онлайн-среде, выделяется ряд признаков, характерных для оффлайн-среды:

1. Увлечения и хобби человека, связанные с оружием, пиротехникой.

2. Наличие у человека холодного, огнестрельного оружия, а также предметов, напоминающих оружие (ножи, топоры, молотки, самопалы, боевое оружие).

3. Большие познания человека в сфере террористических актов, методиках ведения боевых действий, изготовлении оружия, фактов биографий известных преступников.

4. Спортивный или милитари стиль в одежде (спортивные штаны и парка, берцы в сочетании со штанами на подтяжках плюс плащ и т. д.).

5. Присутствие изображений экстремистского и оккультного характера в виде татуировок на теле, рисунков в записях на бумажных и цифровых носителях, предметах одежды и других личных вещах (свастика, портреты Адольфа Гитлера, пентаграммы, изображения сатаны и т. д.), других архаичных божеств из языческой традиции.

6. Следы крови, в том числе застиранной, на предметах одежды и личных вещах человека.

7. Ссадины, синяки, царапины и иные повреждения на теле человека, преимущественно в области кистей рук.

8. Использование в речи аббревиатур и ключевых слов, относящихся к тематике М.К.У.*

9. Использование конспиративных средств связи (мессенджеры Telegram, SureSpot, Adium, Xabber, Jabber, Element и др.)

10. Ночные уединенные прогулки.

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

*Рекомендации по неотложным действиям при выявлении участников движения М.К.У.**

В случае выявления признаков наличия участников движения М.К.У.* в образовательной организации необходимо:

1. Сообщить руководству образовательного учреждения, а также в подразделение полиции по делам несовершеннолетних.

2. Изучить страницы участников движения в социальных сетях и проанализировать размещаемый материал (посты), подписки на группы и страницы, список друзей на предмет отношения к М.К.У.* и другим деструктивным движениям и субкультурам, не вступая в сообщества, не общаясь с участниками.

3. Совместно с правоохранительными органами составить план действий по работе с участниками движения М.К.У.*

4. Привлечь к работе с молодежью по выводу ее из деструктивной среды признанные авторитетные организации (общественные, спортивные, военно-патриотические), молодежных лидеров, спортсменов, представителей силовых структур.

При получении информации о распространении движения вне образовательных учреждений следует совместно с органами правопорядка:

1. Определить возможные «места притяжения» молодежи (спортивные площадки, стадионы, парковые зоны, торгово-развлекательные центры), а также конкретные точки и время сбора лиц (подростков и молодежи) из числа приверженцев М.К.У.*-идеологии.

2. В целях проверки информации и принятия мер профилактического характера информировать о выявленных фактах правоохранительные органы, оказать им содействие в опознании участников движения.

3. Организовать силами местных военно-патриотических объединений и спортивных клубов патрулирование так называемых опасных территорий в темное время суток.

---

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

В случае выявления деструктивного контента, относящегося к М.К.У.*-идеологии, в сети Интернет:

1. Попытаться самостоятельно определить администраторов, модераторов, редакторов группы/паблика/страницы, не подписываясь на сообщества, не общаясь с участниками.

2. Выделить конкретные публикации (посты, рисунки, фото, подписи, комментарии) с признаками деструктивного контента (сцены убийств, издевательств), сделать скриншоты, отправить в правоохранительные органы.

3. Информировать о выявленных страницах М.К.У.*-сообществ органы полиции, НЦПТИ для своевременной их блокировки.

Вопросы и задания для самостоятельной работы

1. Дайте понятие террористическому движению М.К.У.* («Маньяки Культ Убийств»*).

2. Расскажите историю возникновения М.К.У.*

3. В чем заключаются сущность и идеология террористической организации М.К.У.*?

4. Каковы внешние признаки, характерные для участника движения М.К.У.*?

5. Каковы рекомендации по неотложным действиям при выявлении участников движения М.К.У.*?

* Движение признано террористической организацией и запрещено на территории Российской Федерации.

ЗАКЛЮЧЕНИЕ

В контексте глобализации особенности нормативно-правового регулирования общественных отношений определяются посредством спецификации технологий, которые возникли в глобальной сети, например категория «территория» перешла в категорию «трансграничность». Такие технологии, как пиринговые сети, блокчейн, tor-протоколы, анонимные сети, представляют собой распределенную сеть, позволяющую применять вычислительные возможности в разных странах для реализации определенных задач.

Сегодня законодатель должен продумать нормы технического регулирования, согласованные с нормами правового регулирования, поскольку разрушительное программное обеспечение негативным образом воздействует на функционирование киберпространства в контексте глобализации. Подавляющее большинство стран признает информационную безопасность международным и национальным приоритетом, предполагающим анализ информации как объекта правоотношений.

Анализ правовой природы информационной структуры киберсреды в Российской Федерации позволяет выделить ряд характерных черт:

– дефиниция «информационная инфраструктура» констатируется в 50 нормативно-правовых актах Российской Федерации;

– законодатель определяет информационную структуру как континуум искусственной природы, обусловивший ее дифференциацию на государственную, корпоративную или частную разновидности;

– теория информационной инфраструктуры, принятая еще в начале 1990-х годов как политическое кредо, парадигма изыскания информационных векторов, не завершена и в настоящее время и подвержена высокой динамике и симулякратизации;

– с точки зрения российского законодателя, информационные инфраструктуры могут быть представлены в виде симбиоза информационно-телекоммуникационных инфраструктур, сетей связи, а также частных и государственных систем.

Сегодня важно усовершенствовать дефиниции «информация» и «принципы правового регулирования» федерального закона «Об информации, информационных технологиях и о защите информации» с целью упорядочения и гармонизации процессов нормотворчества и правоприменения, в частности правового регулирования информационных отношений в киберсреде (в контексте глобализации). Необходимо дать формальное определение дефиниции «вредная киберинформация» – это сетевой феномен, существующий в киберинформационном пространстве с помощью телекоммуникационный сетей, преднамеренно направленный на разрушение целостности личности, приводящее к самоуничтожению.

Характеризуя концепции правового регулирования киберсреды, отметим, что в этой сфере сосуществуют две амбивалентные концептуальные теории.

Концепция плюрализма правового регулирования Дж. Барлоу представлена в «Декларации независимости киберпространства» как ответ на решение правительства США (1996 г.) ввести цензуру в Интернете.

Регуляционная концепция правового регулирования отношений в киберсреде предлагает превенцию деструктивных, вредных воздействий на личность в виртуальном и реальном мирах.

Исходя из принципа паритетности, мировое сообщество осознает, что, опираясь на принцип справедливости, каждый субъект имеет право на аргументацию своей теории. Выход из непростой ситуации видится в соблюдении принципа законности. Не только Российская Федерация, но и многие страны Европы, США пытаются обогатить национальное право для совершенствования государственной безопасности информационного пространства и защиты государственных интересов от деструктивного воздействия информации и глобальных рисков.

Специфика национального правового обеспечения информационной безопасности и киберпространства опирается на понимание, что использование блокчейн-технологий, кибервалюты, информационной государственной многофункциональной телекоммуникационной инфраструктуры, частных облачных хранилищ, прокси-серверов, IOT, IT невозможно без правового регулирования всеми участниками киберинформационной системы (ООН, ЕЕ, ОЭСР, СНГ).

Для противодействия деструктивной информации в сети Интернет в процессе применения дифференцированных ИТ распределительных технологий необходимо правовое обеспечение. В ином случае это приведет к информационным рискам, связанным с безопасностью государств, а также большого количества пользователей, использующих разные онлайн-сервисы.

Таким образом, в учебном пособии представлены мнения современных исследователей цифрового права и предложены сформулированные закономерности государственного правового регулирования информационных отношений в киберсреде:

– ориентация на международные договоры;

– международное сотрудничество;

– правовое регулирование (поиск и удаление) вредной киберинформации в глобальном пространстве.

Особенности правового регулирования информационных отношений в киберсреде в контексте глобализации позволяют на основе вышеизложенного сформулировать предложения для совершенствования информационного законодательства. Следует отметить, что данная проблема дифференцирована и многоаспектна, чтобы быть решенной в короткие сроки и с незначительными затратами. Необходимо усовершенствовать правовое регулирование информационных отношений, в частности, дополнив дефиницию «информация». Важно установить правовые основы межгосударственного взаимодействия с привлечением независимых экспертов, для того чтобы максимально ограничить вовлечение таких специалистов в процессы санкциональной блокировки тех или иных информационных систем, серверов заинтересованными структурами, в том числе государственными.

Немало вопросов вызывает такой аспект, как приоритет национального правового регулирования деятельности транснациональных проектов, организаций, юридических и физических лиц. Таким образом, получается, что провайдеры на абсолютно законных основаниях могут хранить вредную киберинформацию или заблокировать экономический сервер в IOT. С целью упорядочения и гармонизации процессов нормотворчества и правоприменения, в частности правового регулирования информационных отношений в киберсреде (в контексте глобализации), предлагается введение принципа интероперабельности в ст. 3 (Принципы правового регулирования отношений в сфере

информации, информационных технологий и защиты информации) федерального закона «Об информации, информационных технологиях и о защите информации».

Особенности правового регулирования информационных отношений в киберсреде (в глобальном контексте) создают необходимость упорядочивания определения критериев киберсреды. К ним относятся: универсальность, транснациональность, атерриториальность, переходность, динамизм, глобализм, внегосударственность. Применение принципа интероперабельности создает новые возможности стандартизации систем, их открытости и интеграции с актуальными ИТ, что может сократить противоречия и путаницу в правовом регулировании информационных отношений в этом секторе.

В учебном пособии представлен анализ современных экстремистских и террористических организаций, запрещенных на территории Российской Федерации, чья деятельность ведется в информационно-коммуникационной сети Интернет, и способы действий при их выявлении.

Следует подчеркнуть, что самостоятельно, без участия правоохранительных органов и экспертов работать с группами аутодеструктивной, экстремистской и террористической направленности не рекомендуется.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативные правовые акты

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 г. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.09.2021).

2. Гражданский кодекс Российской Федерации. Часть первая от 30 нояб. 1994 г. № 51-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.09.2021).

3. О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы [Электронный ресурс] : указ президента Рос. Федерации от 09 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. – 2017. – № 20. – Ст. 2901. – URL: https://www.szrf.ru/ (дата обращения: 22.01.2021).

4. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации : федер. закон Рос. Федерации от 31 июля 2020 г. № 259-ФЗ. – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01.09.2021).

5. Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры [Электронный ресурс] : постановление Правительства Рос. Федерации от 8 июня 2019 г. № 743 // Собрание законодательства Российской Федерации. – 2019. – № 24. – Ст. 3099. – URL: https://www.szrf.ru/ (дата обращения: 22.01.2021).

6. О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено» (вместе с «Правилами создания, формирования и ведения единой автоматизированной информационной системы “Единый реестр доменных имен, ука-

зателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено”», «Правилами принятия уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти решений в отношении отдельных видов информации и материалов, распространяемых посредством информационно-телекоммуникационной сети “Интернет”, распространение которых в Российской Федерации запрещено») : постановление Правительства Рос. Федерации от 26 окт. 2012 г. № 1101 (ред. от 12 окт. 2021 г.). – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01. 09.2021).

7. Об определении официальных сайтов в информационно-телекоммуникационной сети «Интернет» оператора единого реестра российских программ для электронных вычислительных машин и баз данных и оператора единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации [Электронный ресурс] : приказ Минкомсвязи России от 11 июня 2019 г. № 278 // Официальный интернет-портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 01. 09.2021).

8. Прогноз научно-технологического развития Российской Федерации на период до 2030 года [Электронный ресурс] : утв. Правительством Рос. Федерации // Собрание законодательства Рос. Федерации. – 2018. – № 42 (ч. II). – Ст. 6480. – URL: https://www.szrf.ru/ (дата обращения: 22.01.2021).

9. Методика определения количества пользователей сайта или страницы сайта в сети Интернет [Электронный ресурс] : утв. Роскомнадзором. – URL: http://rk№.gov.ru/№ ews/ rsoc/ № ews26519.htm (дата обращения: 19. 02.2019).

10. Документы в области метрологии : указатель / Федер. агентство по техн. регулированию и метрологии; сост. : П. К. Одинцов [и др.]. – М. : Стандартинформ, 2020. – 240 с.

Нормативные правовые акты иностранных государств

11. Декларация лидеров G20 – программный документ построения современного Вавилона на основе внедрения цифровых технологий [Электронный ресурс]. – URL: https://a№ tieres.wordpress.com/2017/07/13/valerij_filimo№ov_deklaratsija_sammita_g20_v_gamburge_postroje№ie_vavilo№a_№a_os№ove_tsifrovih_teh№ologiy/ (дата обращения: 19.10.2018).

12. Конвенция о преступности в сфере компьютерной информации (ETS № 185). – Доступ из справ.-правовой системы «КонсультантПлюс» (дата обращения: 01. 09.2021).

13. Концепция формирования информационного пространства СНГ [Электронный ресурс] // Официальный сайт СНГ. – URL: http://www.cis.mi№sk.by/page.php?id=7548 (дата обращения: 19.02.2019).

14. Резолюция, принятая Генеральной Ассамблеей 21 дек. 2009 г. (по докладу Второго комитета (A/64/422/Add.3)] 64/211. Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур) [Электронный ресурс] // Организация Объединенных Наций A/RES/64/211. – URL: https://undocs.org/ru/A/RES/64/211 (дата обращения: 14.10.2020).

15. Резолюции ГА 723 (VIII) от 23 окт. 1953 г. и ECOSOC резолюции 1199 (XLII) 24 мая 1967 г. [Электронный ресурс]. – URL: https://publicadministration.un.org/ru/About-Us/Who-We-Are (дата обращения: 27.05.2020).

Монографии, учебные пособия

16. *Бачило, И. Л.* Природа информационных конфликтов. Конфликты в информационной сфере и их причины / И. Л. Бачило // Конфликты в информационной сфере: правовые аспекты : материалы теорет. семинара Сектора информац. права, 2008 г. / под ред. И. Л. Бачило. – М. : [б. и.], 2009. – С. 36 – 50.

17. *Бачило, И. Л.* Информационное право : учеб. для вузов / И. Л. Бачило. – 5-е изд., перераб. и доп. – М. : Юрайт, 2022. – 419 с.

18. *Головкин, Р. Б.* Актуальные проблемы теории правового регулирования / Р. Б. Головкин, Ю. П. Колесникова, О. Д. Третьякова. – 2-е изд., стер. – М. : Юрайт, 2020. – 305 с.

19. *Городов, О. А.* Информационное право : учеб. для бакалавров / О. А. Городов. – М. : Проспект, 2016. – 304 с.

20. *Жарова, А. К.* Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации : монография / А. К. Жарова. – М. : Юрайт, 2021. – 301 с.

21. *Жарова, А. К.* Информация. Правовые проблемы обращения информации / А. К. Жарова. – М. : Янус, 2006. – 208 с.

22. *Керимов, Д. А.* Методология права: предмет, функции, проблемы философии права : монография / Д. А. Керимов. – 3-е изд., перераб. и доп., репр. изд. – М. : Норма : ИНФРА-М, 2020. – 524 с.

Научные статьи

23. *Башлыкова, А. А.* Решение проблемы интероперабельности в проектах «Умного города» / А. А. Башлыкова, А. Я. Олейников, Т. А. Гаджикулыев // Современные информационные технологии и ИТ-образование. – 2019. – V. 5. – № 3. – DOI: 10.25559^тТО. 15.201903.767-774.

24. *Богданов, Е. В.* Информация как объект гражданских правоотношений / Е. В. Богданов // Гражданское право. – 2018. – № 5. – С. 29 – 33.

25. *Грибанов, Д. В.* Деятельность субъектов общественного контроля и развитие систем распределенных вычислений и распределенного хранения данных / Д. В. Грибанов // Право и управление. XXI век. – 2018. – № 1 (46). – С. 14 – 22.

26. *Жарова, А. К.* Международные правовые концепции борьбы с распространением вредной информации / А. К. Жарова // Бизнес-информатика. – 2010. – № 4. – С. 46 – 53.

27. *Жарова, А. К.* Условия оказания услуги по предоставлению доступа к облачным вычислениям / А. К. Жарова // Государство и право. – 2012. – № 12. – С. 86 – 90.

28. *Жарова, А. К.* О правовом регулировании технологического обеспечения информационного взаимодействия субъектов / А. К. Жарова // Труды института государства и права. – 2012. – № 3. – С. 186 – 199.

29. *Исаков, В. Б.* Правовые аспекты внедрения интернета вещей / В. Б. Исаков, В. К. Сарьян, А. А. Фокина // ИТ-Стандарт. – 2015. – № 4 (5). – С. 9 – 16.

30. *Кириченко, О. В.* Информация как объект гражданских правоотношений / Р. В. Кириченко // Современное право. – 2014. – № 9. – С. 77 – 81.

31. *Лопатин, В. Н.* Проблемы правовой защиты человека в информационной войне / В. Н. Лопатин // Информационное право. – 2014. – № 6 (42). – С. 17 – 24.

32. *Минбалеев, А. В.* Место и роль саморегулирования в развитии цифровых технологий / А. В. Минбалеев // Образование и право. – 2019. – № 1. – С. 253 – 256.

33. *Минбалеев, А. В.* Правовое обеспечение кибербезопасности во Вьетнаме / А. В. Минбалеев // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 1 (31). – С. 64 – 68.

34. *Недорезков, В. В.* Криптовалюты на базе технологии блокчейна: проблемы правового регулирования / В. В. Недорезков // Банковское право. – 2017. – № 4. – С. 45 – 49.

35. *Олейников, А. Я.* Проблема интероперабельности в Вооруженных силах РФ / А. Я. Олейников, И. И. Чусов // Вестник Академии военных наук. – 2017. – № 4 (61). – С. 61 – 68.

36. *Савенков, А. Н.* Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности / А. Н. Савенков // Государство и право. – 2017. – № 10. – С. 5 – 18.

ПРИЛОЖЕНИЯ

Приложение 1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ «НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ)

Педагогический институт

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ»

Направление подготовки 44.03.05 «Педагогическое образование»

г. Владимир
2025

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цели освоения дисциплины «Нормативно-правовое обеспечение профессиональной деятельности»:

– дать обзор основных понятий об образовательных отношениях, отражающих специфику взаимоотношений личности, общества и государства в сфере образования и представляющих собой самостоятельный вид общественных и правовых отношений;

– сформировать у студентов умения и навыки анализа всех системных компонентов образовательного права – предмета, метода и правового режима;

– познакомить с современными тенденциями, информационно-коммуникативной культурой, различными аспектами правового регулирования образовательной системы;

– изучить нормы международного законодательства в области обеспечения прав человека на образование, российского законодательства и субъектов Российской Федерации в области регулирования образовательных отношений.

Задачи:

– помочь студентам получить знания об особенностях регламентации правовых отношений в сфере образования в России;

– сформировать правовую культуру, развить навыки работы с нормативно-правовыми документами, необходимыми в образовательной сфере;

– изучить понятия, основные источники, предмет и пределы правового регулирования отношений в сфере образования, которые в дальнейшем могут быть использованы при освоении смежных дисциплин;

– активизировать интерес к актуальным проблемам правового регулирования и стремление к повышению уровня профессиональной подготовки специалистов в образовании;

– сформировать у студентов информационно-коммуникативную культуру;

– воспитать интолерантность к терроризму, экстремизму и коррупционной деятельности;

– сформировать навыки профилактики противодействия идеологии терроризма, коррупции и профилактики экстремистских явлений.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Нормативно-правовое обеспечение профессиональной деятельности» относится к обязательной части.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Таблица 1

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемая компетенция (код, содержание компетенции)	Планируемые результаты обучения по дисциплине в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих норм, имеющихся ресурсов и ограничений	УК-2.1. Формулирует в рамках поставленной цели проекта совокупность взаимосвязанных задач, обеспечивающих ее достижение. Определяет ожидаемые результаты решения выделенных задач, действующих правовых норм. УК-2.2. Проектирует решение конкретной задачи проекта, выбирая оптимальный способ ее решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений. УК-2.3. Решает конкретные задачи проекта, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, заявленного качества и за установленное время. УК-2.4. Публично представляет результаты решения конкретной задачи проекта, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	*Знает:* – принципы и методы декомпозиции задач, действующие правовые нормы; – принципы и методы анализа имеющихся ресурсов и ограничений. *Умеет:* – определять круг задач в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; – выбирать оптимальные способы решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений. *Владеет:* – практическими навыками определения круга задач в рамках поставленной цели, исходя из действующих правовых норм, имеющихся ресурсов и ограничений; – практическими навыками выбора оптимальных способов решения задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.	1. Тестовые вопросы. 2. Ситуационные задачи. 3. Практико-ориентированное задание. 4. Киберквесты. 5. Мультимедийные минипроекты.

Продолжение табл. 1

Формируемая компетенция (код, содержание компетенции)	Планируемые результаты обучения по дисциплине в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	
УК-10. Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.1. Знает признаки экстремистской, террористической и коррупционной деятельности, действующие правовые нормы в сфере противодействия экстремизму, терроризму, коррупции. УК-10.2. Умеет планировать, организовывать и проводить мероприятия, обеспечивающие формирование нетерпимого отношения к проявлениям экстремизма, терроризма, коррупционного поведения. УК-10.3. Владеет навыками противодействия различным проявлениям коррупционного поведения, экстремизма и терроризма в профессиональной деятельности.	*Знает:* – действующие правовые нормы, регламентирующие противодействие проявлениям терроризма, экстремизма и коррупции в различных областях жизнедеятельности, в том числе в киберсреде. *Умеет:* – планировать, организовывать и проводить мероприятия, обеспечивающие формирование гражданской позиции противодействия идеологии терроризма и профилактику проявлений экстремизма и коррупции в социуме, в том числе в киберсреде. *Владеет:* – навыками информационно-коммуникативной культуры в обществе на основе *нетерпимого отношения к проявлениям терроризма, кибертерроризма, экстремизма, киберэкстремизма и коррупции*; – способами мониторинга киберпространства на предмет выявления и проведения профилактики киберпреступлений.	1. Тестовые вопросы 2. Ситуационные задачи 3. Киберквесты 4. Практико-ориентированное задание 5. Мультимедийные мини-проекты

Окончание табл. 1

Формируемая компетенция (код, содержание компетенции)	Планируемые результаты обучения по дисциплине в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции (код, содержание индикатора)	Результаты обучения по дисциплине	
ОПК-1. Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики	ОПК. 1.1. Демонстрирует знания нормативно-правовых актов в сфере образования и нормы профессиональной этики. ОПК. 1.2. Строит образовательный процесс в соответствии с правовыми и этическими нормами профессиональной деятельности. ОПК. 1.3. Организует образовательную среду в соответствии с правовыми и этическими нормами профессиональной деятельности.	*Знает:* – международные стандарты в области защиты прав человека и гражданина, прав ребёнка, инвалидов и лиц с ограниченными возможностями здоровья; – систему и источники законодательства о труде Российской Федерации, включая конвенции МОТ. *Умеет*: – анализировать и практически использовать нормативно-правовые акты в области образования и оценивать качество образовательных услуг на основе действующих нормативно-правовых актов. *Владеет:* – навыками работы с законодательными и иными нормативно-правовыми актами в области образования; – способами решения проблем правового обеспечения профессиональной деятельности в современных условиях.	1. Тестовые вопросы 2. Ситуационные задачи 3. Киберквесты 4. Практико-ориентированное задание 5. Мультимедийные мини-проекты

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа.

Таблица 2

Тематический план
(форма обучения – очная)

Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			Лекции	Практические занятия	Лабораторные работы	В форме практической подготовки		
Тема 1. Актуальные правовые проблемы в сфере образовательных отношений в Российской Федерации.	3	1	2	2			2	
Тема 2. Организация противодействия идеологии терроризма в Российской Федерации (в соответствии с Комплексным планом противодействия идеологии терроризма в Российской Федерации).	3	2	2	2			6	
Тема 3. Государственная политика в области образования, ее правовая регламентация. Меры по формированию у молодежи антитеррористического сознания и информационно-коммуникативной культуры.	3	3 – 4	2				2	Рейтинг-контроль № 1

Окончание табл. 2

Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			Лекции	Практические занятия	Лабораторные работы	В форме практической подготовки		
Тема 4. Создание позитивного контента в системе противодействия распространению идеологии терроризма, экстремизма в киберсреде. Практика разработки профилактических психолого-педагогических методических материалов по противодействию экстремизму и терроризму в молодежной среде.	3	5		2			2	
Тема 5. Нормативно-правовые и организационные основы деятельности образовательных учреждений.	3	6 – 10	4	4			8	
Тема 6. Образовательные стандарты: виды, сравнение, отличия.	3	11 – 12	2	2			4	Рейтинг-контроль № 2
Тема 7. Образовательное право России в мировом образовательном пространстве: актуальные проблемы развития.	3	13 – 14	2	2			4	
Тема 8. Законодательные акты Российской Федерации по противодействию коррупции: актуальные проблемы правоприменительной практики в сфере образования.	3	15 – 16	2	2			4	
Тема 9. Уголовно-правовая характеристика коррупционных преступлений в образовании. Специфика организации антитеррористической защищённости (АТЗ) в образовательной организации.	3	17 – 18	2	2			4	Рейтинг-контроль № 3
Всего за 3-й семестр		**1 – 18**	**18**	**18**			**36**	**Зачет**
Наличие в дисциплине КП/КР				–				–
Итого по дисциплине			**18**	**18**			**36**	**Зачет**

5. СОДЕРЖАНИЕ ЛЕКЦИОННЫХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

Тема 1. Актуальные правовые проблемы в сфере образовательных отношений в Российской Федерации.

Основные законодательные акты в области образования. Источники образовательного права. Характеристика образовательных отношений, управление системой образования. Права ребенка и формы правовой защиты в законодательстве Российской Федерации. Основные положения нормативно-правовых актов Российской Федерации в сфере противодействия экстремизму и терроризму.

Тема 2. Организация противодействия идеологии терроризма в Российской Федерации (в соответствии с Комплексным планом противодействия идеологии терроризма в Российской Федерации).

Особенности организации и проведения мероприятий, направленных на развитие у детей и молодежи неприятия идеологии терроризма и привитие им традиционных российских духовно-нравственных ценностей. Вопросы учебно-методического сопровождения реализации мероприятий, направленных на противодействие идеологии терроризма. Опыт государственных, общественных и религиозных организаций Российской Федерации по профилактике противодействия идеологии терроризма.

Три уровня террористической опасности, порядок их установления, знакомство с комплексом действий, необходимых на практике для реализации мероприятий, соответствующих установленному уровню террористической опасности.

Организация мониторинга политических социально-экономических и иных процессов, оказывающих влияние на ситуацию в области терроризма.

Роль и место антитеррористических комиссий в субъектах Российской Федерации и муниципальных образований в противодействии идеологии терроризма.

Профилактическая работа с молодежью, в том числе с лицами, состоящими на профилактическом учете и (или) находящимися под административным надзором в органах внутренних дел Российской Федерации в связи с причастностью к совершению правонарушений в сфере общественной безопасности, в форме индивидуальных (групповых) бесед по формированию стойкого неприятия идеологии терроризма и привитию традиционных российских духовно-нравственных ценностей.

Тема 3. Государственная политика в области образования, ее правовая регламентация. Меры по формированию у молодежи антитеррористического сознания и информационно-коммуникативной культуры.

Роль государства в становлении и развитии образования. Принципы государственной образовательной политики. Принципы работы с информационными ресурсами в киберсреде.

Воспитательные и культурно-просветительские мероприятия, направленные на развитие у детей и молодежи неприятия идеологии терроризма и привитие им традиционных российских духовно-нравственных ценностей на базе образовательных организаций.

Информационные и методические материалы по развитию у детей и молодежи неприятия идеологии терроризма и привитию традиционных российских духовно-нравственных ценностей. Правовые основы формирования у учащихся основ информационной безопасности, в том числе по вопросам защиты детей от пропаганды идеологии терроризма и экстремизма при использовании сети Интернет.

Правовые основы формирования информационно-коммуникативной культуры. Методические рекомендации для федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления по профилактике распространения радикальной идеологии среди верующих.

Тема 4. Создание позитивного контента в системе противодействия распространению идеологии терроризма, экстремизма в киберсреде. Практика разработки профилактических психолого-педагогических методических материалов по противодействию экстремизму и терроризму материалов в молодежной среде.

Создание позитивного контента в системе профилактики распространения идеологии терроризма, экстремизма в киберсреде в образовательной организации.

Принципы формирования информационно-коммуникативной культуры обучающихся. Возможности симулякративного подхода в противодействии кибертерроризму и киберэкстремизму.

Система профилактических мер, направленных на нераспространение идеологии экстремизма и терроризма в сети Интернет.

Информационные и воспитательные мероприятия, направленные на предупреждение распространения деструктивного контента в сети Интернет.

Работа с нормативно-правовыми документами. Анализ российского и международного законодательства, регулирующего ответственность за участие в деятельности экстремистских/террористических/деструктивных молодежных движений (субкультур).

Тема 5. Нормативно-правовые и организационные основы деятельности образовательных учреждений.

Понятие «образовательное учреждение». Типы и виды образовательных учреждений. Права, обязанности, ответственность образовательных учреждений. Образовательные правоотношения в системе непрерывного образования. Особенности правового регулирования в сфере образования на различных его ступенях.

Тема 6. Образовательные стандарты: виды, сравнение, отличия.

Понятие государственного образовательного стандарта. Порядок разработки, утверждения и введения в действие государственных

образовательных стандартов. Образовательные стандарты первого, второго, третьего поколения. Федеральные государственные образовательные стандарты. Различие между образовательными стандартами общего и профессионального образования. Соотношение образовательного стандарта и образовательной программы. Порядок формирования основных образовательных программ. Академические свободы вуза при реализации основных образовательных программ.

Тема 7. Образовательное право России в мировом образовательном пространстве: актуальные проблемы развития.

Основные правовые акты международного образовательного законодательства. Соотношение российского и зарубежного законодательства в области образования. Нормативно-правовое обеспечение модернизации российского педагогического образования.

Тема 8. Законодательные акты Российской Федерации по противодействию коррупции: актуальные проблемы правоприменительной практики в сфере образования.

Законодательные акты Российской Федерации по противодействию коррупции: основные положения. Роль федерального закона от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции». Основные принципы противодействия коррупции:

1) признание, обеспечение и защита основных прав и свобод человека и гражданина;

2) законность;

3) публичность, открытость деятельности государственных органов и органов местного самоуправления;

4) неотвратимость ответственности за совершение коррупционных правонарушений;

5) комплексное использование политических, организационных, информационно-пропагандистских, социально-экономических, правовых, специальных и иных мер;

6) приоритетное применение мер по предупреждению коррупции;

7) сотрудничество государства с институтами гражданского общества, международными организациями и физическими лицами.

Организационные основы противодействия коррупции. Меры по профилактике коррупции. Основные направления деятельности государственных органов по повышению эффективности противодействия коррупции.

Тема 9. Уголовно-правовая характеристика коррупционных преступлений в образовании. Специфика организации АТЗ в образовательной организации.

Определение должностного лица в уголовном законодательстве. Деструктивное влияние коррупционных преступлений на нормальное функционирование и развитие экономики. Взаимосвязь коррупционных преступлений с иными видами преступной деятельности. Объективные и субъективные признаки некоторых видов коррупционных преступлений.

Злоупотребление должностными полномочиями: понятие, признаки, вопросы квалификации (ст. 285 УК РФ). Превышение должностных полномочий (ст. 286 УК РФ).

Условия, определяющие уголовную ответственность за эти преступления. Социально-правовые условия и проблемы криминализации взяточничества. Получение взятки (ст. 290 УК РФ). Понятие взятки. Формы использования лицом, получившим взятку, своего служебного положения. Обстоятельства, отягчающие уголовную ответственность за получение взятки.

Особенности квалификации рассматриваемого преступления, совершенного в соучастии, с вымогательством предмета взятки и в крупном размере. Дача взятки: основной и квалифицированный составы преступления (ст. 291 УК РФ).

Злоупотребление полномочиями лицом, выполняющим управленческие функции в коммерческой или иной организации (ст. 201 УК РФ). Коммерческий подкуп (ст. 204 УК РФ). Понятие и формы коммерческого подкупа. Предмет преступления. Квалифицирующие признаки. Роль постановлений Пленума Верховного суда Российской Федерации в формировании уголовно-правовой характеристики коррупционных преступлений.

6. СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ

Тема 1. Актуальные правовые проблемы в сфере образовательных отношений в Российской Федерации.

План

1. Конституция Российской Федерации как основа правового регулирования в сфере образования.
2. Нормативно-правовое обеспечение в сфере образования.
3. Федеральный закон «Об образовании в Российской Федерации».
4. Структура системы образования. Уровни образования. Профессиональные образовательные стандарты.
5. Смежные законодательные и подзаконные нормативные акты, затрагивающие область образования: Трудовой кодекс РФ, Гражданский кодекс РФ, Налоговый кодекс РФ, Бюджетный кодекс РФ.
6. Типовые положения об образовательных учреждениях.
7. Основные положения Конвенции о правах ребенка и закона Российской Федерации «Об основных гарантиях прав ребенка в Российской Федерации».
8. Права ребенка и формы их правовой защиты.
9. Оказание практической правовой помощи в области социальной защиты, осуществление сотрудничества с органами правопорядка и органами социальной защиты населения.
10. Формы работы с родителями, направленные на правовое просвещение.

Методические рекомендации

1. В тетрадях для практических занятий проанализируйте термины, которые нормативно определены законом об образовании для использования в работе общеобразовательного учреждения (сущностный анализ трактовки совместно с преподавателем терминов: *образование, воспитание, обучение, федеральный государственный образовательный стандарт, образовательная программа, примерная основная образовательная программа, общее образование, качество образования).*

2. Ознакомьтесь с текстом закона об образовании.

3. Составьте конспект-схему на тему: «Направленность каждой главы закона об образовании».

4. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 2. Организация противодействия идеологии терроризма в Российской Федерации (в соответствии с Комплексным планом противодействия идеологии терроризма в Российской Федерации).

План

1. Общие положения об исполнении мероприятий Комплексного плана противодействия идеологии терроризма в Российской Федерации.

2. Структура и содержание Комплексного плана противодействия идеологии терроризма в Российской Федерации.

3. Социально-экономические меры, предусмотренные законодательством Российской Федерации, в отношении лиц, отбывших наказание за совершение преступлений террористического характера, направленные на их ресоциализацию.

4. Информационно-пропагандистские мероприятия по разъяснению преступной сущности и общественной опасности терроризма.

5. Профилактическая работа с молодежью, в том числе с лицами, состоящими на профилактическом учете и (или) находящимися под административным надзором в органах внутренних дел Российской Федерации в связи с причастностью к совершению правонарушений в сфере общественной безопасности, в форме индивидуальных (групповых) бесед по формированию стойкого неприятия идеологии терроризма и привитию традиционных российских духовно-нравственных ценностей.

6. Мероприятия по доведению до лиц, прибывающих из стран с повышенной террористической активностью для временного проживания и осуществления трудовой деятельности на территории Россий-

ской Федерации, норм законодательства Российской Федерации, устанавливающих ответственность за участие и содействие террористической деятельности, разжигание социальной, расовой, национальной и религиозной розни, создание и участие в подобной деятельности.

Методические рекомендации

1. Ознакомьтесь с Комплексным планом противодействия идеологии терроризма в Российской Федерации на 2024 – 2025 годы.

2. Составьте план мероприятия (см. п. 1). Какие три даты подходят для реализации плана?

3. Составьте цикл мероприятий согласно п. 2. Какие формы работы можно выбрать?

4. Составьте конспект-схему на тему «Реализация мероприятий Комплексного плана».

Тема 3. Государственная политика в области образования, ее правовая регламентация. Меры по формированию у молодежи антитеррористического сознания и информационно-коммуникативной культуры.

План

1. Государственная политика в области образования, ее правовая регламентация.
2. Роль государства в становлении и развитии образования.
3. Принципы государственной образовательной политики.
4. Конституционное право граждан на образование.
5. Правовая регламентация приема в образовательное учреждение.
6. Государственные гарантии приоритетности образования.
7. Право на образование: проблемы его реализации.
8. Система государственных органов, обеспечивающих исполнение обязательств государства в сфере образования.
9. Государственно-общественные объединения и общественные организации в системе образования. Понятие и признаки образовательных отношений. Отношения в сфере образования.
10. Отношения между органами государственной власти и ее субъектами, органами местного самоуправления. Их полномочия и компетенции в системе управления образованием.

11. Правовые механизмы формирования антитеррористического сознания.

12. Как сформированная информационно-коммуникативная культура способствует противодействию кибертерроризму?

13. Анализ российского и международного законодательства, регулирующего ответственность за участие в деятельности экстремистских/террористических/деструктивных молодежных движений (субкультур).

14. Анализ российского и международного законодательства, регулирующего ответственность за участие в деятельности движений криминальной направленности.

Методические рекомендации

1. Представьте в виде таблицы общие требования к приему граждан в образовательные учреждения и организации образовательного процесса, а также основные типы обучения.

2. Составьте конспект-схему «Правовые основы управления государственными и муниципальными образовательными учреждениями, а также негосударственными образовательными учреждениями».

3. Проанализируйте принципы государственной образовательной политики.

4. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 4. Создание позитивного контента в системе противодействия распространению идеологии терроризма, экстремизма в киберсреде. Практика разработки профилактических психолого-педагогических методических материалов по противодействию экстремизму и терроризму материалов в молодежной среде.

План

1. Создание позитивного контента в системе профилактики распространения идеологии терроризма, экстремизма в киберсреде в образовательной организации.

2. Принципы формирования информационно-коммуникативной культуры обучающихся.

3. Возможности симулякративного подхода в противодействии кибертерроризму и киберэкстремизму.

4. Система профилактических мер, направленных на нераспространение идеологии экстремизма и терроризма в сети Интернет.

5. Информационные и воспитательные мероприятия, направленные на предупреждение распространения деструктивного контента в сети Интернет.

6. Анализ российского и международного законодательства, регулирующего ответственность за участие в деятельности экстремистских/террористических/деструктивных молодежных движений (субкультур).

7. Основные законодательные и иные правовые акты Российской Федерации в сфере противодействия экстремизму.

8. Содержание молодежной политики в сфере профилактики экстремизма.

9. Сущность сетевых движений радикальной направленности и деструктивных субкультур терминальной направленности.

10. Сравнение деструктивного поведения с делинквентным.

11. Основные движения криминальной направленности, действующие на территории Российской Федерации.

12. Идеология движения криминальной направленности АУЕ*.

13. Сетевое молодежное движение террористической направленности «скулшутинг»** («колумбайн»**).

14. Сетевое молодежное движение террористической направленности М.К.У.**.

15. Характеристика контента движений, продвигающих аутодеструктивное поведение, размещенного в сети Интернет.

16. Механизмы формирования и распространения деструктивного поведения подростков и молодежи.

Методические рекомендации

В тетради для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

---

* Признано экстремистской организацией и запрещено на территории Российской Федерации.

** Признано террористической организацией и запрещено на территории Российской Федерации.

Тема 5. Нормативно-правовые и организационные основы деятельности образовательных учреждений.

План

1. Правовой статус образовательных учреждений.
2. Филиалы, отделения, структурные подразделения образовательных учреждений, объединения, союзы, ассоциации. Регламентация их деятельности.
3. Учредительные документы, регистрация, лицензирование, аттестация, аккредитация образовательных учреждений.
4. Автономия образовательных учреждений.
5. Типовые положения о соответствующих типах и видах образовательных учреждений. Требования к уставу образовательного учреждения, его правовой статус.
6. Учредители образовательных учреждений и организаций. Определение правоотношений между учредителем и образовательным учреждением или образовательной организацией.
7. Защита прав и законных интересов образовательных учреждений.
8. Ответственность образовательного учреждения перед личностью, обществом, государством. Контроль за соответствием деятельности образовательного учреждения целям, предусмотренным его уставом.
9. Органы управления образовательных учреждений.
10. Нормативно-правовое обеспечение взаимодействия систем общего и профессионального образования.

Методические рекомендации

1. В тетрадях для практических занятий изложите сущность понятий: *непрерывное образование, дополнительное образование*.
2. Выделите основные формы защиты прав работников образовательных учреждений, особенности правового регулирования общего, профессионального, дополнительного образования и профессионального обучения.
3. Представьте в виде таблицы формы непрерывного образования.

4. Назовите и охарактеризуйте специфику правового регулирования трудовых, имущественных, управленческих отношений в образовательных учреждениях различных типов и видов.

5. Назовите и охарактеризуйте основные особенности правового регулирования трудовых отношений в области образования и оплаты труда.

6. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Вопросы, выносимые на обсуждение в форме круглого стола

1. Правовое регулирование отношений в сфере общего образования.

2. Правовое регулирование отношений, связанных с получением образования в семье.

3. Правовое регулирование отношений, связанных с образованием и воспитанием детей-сирот и детей, оставшихся без попечения родителей.

4. Правовое регулирование отношений, связанных с получением образования лицами с ограниченными возможностями здоровья.

5. Особенности реализации общеобразовательных программ дополнительного образования.

6. Правовой статус учащихся образовательных учреждений. Социальная защита учащихся. Права и обязанности родителей (законных представителей) в образовательных отношениях.

7. Особенности правового обеспечения профессиональной педагогической деятельности. Правовой статус работников общеобразовательных учреждений.

Тема 6. Образовательные стандарты: виды, сравнение, отличия

План

1. Структура и содержание ФГОС основного общего образования 1, 2, 3-го поколений.

2. Особенности ФГОС основного общего образования 1, 2, 3-го поколений.

3. Структура и содержание ФГОС ВО 3+ и ФГОС ВО 3++.

4. Организация учебного процесса и формы обучения по стандартам 1-го и 2-го поколений.

5. Организация учебного процесса и формы обучения по стандартам ФГОС ВО 3+ и ФГОС ВО 3++.

6. Что такое профессиональный и образовательный стандарты?

7. Различие профессиональных и образовательных стандартов.

8. Проблема взаимосвязи профессионального и образовательного стандартов.

Методические рекомендации

1. В тетрадях для практических занятий изложите сущность понятий: *бакалавр* (как степень), *магистр* (как степень), *квалификация высшего образования, направление подготовки, направленность образовательной программы, компетенция, профиль, дидактическая единица, зачетная единица, программа учебной дисциплины*.

2. Изучите федеральный государственный образовательный стандарт. Укажите его основные структурные компоненты и дайте им краткую характеристику. Заполните таблицу.

3. По своему направлению обучения определите:

– область профессиональной деятельности;

– объекты профессиональной деятельности;

– виды и задачи профессиональной деятельности.

4. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 7. Образовательное право России в мировом образовательном пространстве: актуальные проблемы.

План

1. Зарубежные образовательные системы и направления их реформирования.

2. Обновление содержания образования. Структурные изменения образовательных систем. Система финансирования как экономический рычаг управления образованием.

3. Привлечение к управлению образованием общественных организаций. Формирование европейского образовательного пространства.

4. Основные правовые акты международного образовательного законодательства. Документы ООН (Всеобщая декларация прав человека, Конвенция о правах ребенка).

5. Основные правовые акты международного образовательного законодательства. Документы ЮНЕСКО (Конвенция о борьбе с дискриминацией в области образования, Рекомендации о борьбе с дискриминацией в области образования, рекомендации МОТ/ЮНЕСКО о положении учителей, рекомендации о статусе преподавательских кадров учреждений высшего образования).

6. Нормативно-правовые акты систем образования стран СНГ.

7. Проблемы соотнесения образовательных систем стран СНГ и российской образовательной системы.

8. Интеграция образования Российской Федерации в мировую образовательную систему.

9. Нормативно-правовая поддержка вхождения Российской Федерации в Болонский процесс.

10. Основные задачи модернизации педагогического образования. Обновление нормативно-правового, научного и учебно-методического обеспечения педагогического образования.

Методические рекомендации

1. В тетрадях для практических занятий изложите сущность понятий: *профессиональная деятельность, педагогическая деятельность, педагогическое общение.*

2. Охарактеризуйте педагогическую деятельность.

3. Назовите и опишите основные педагогические умения.

4. Выделите специфику педагогического общения, его отличие от общения.

5. Составьте конспект-схему «Знания, умения и профессионально важные качества личности учителя истории».

6. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Вопросы, выносимые на обсуждение в форме круглого стола

1. Создание механизмов эффективно и динамично функционирующей системы педагогического образования.

2. Оптимизация структуры и совершенствование организации профессиональной подготовки педагогов.

3. Модернизация педагогического образования как основа совершенствования системы общего образования с учетом новых социальных требований к образовательной системе.

4. Обновление структуры и содержания общего образования, использование эффективных методов воспитания и обучения.

5. Сравнительный анализ подготовки педагогических кадров и их материального обеспечения в России и других странах.

Тема 8. Законодательные акты Российской Федерации по противодействию коррупции: актуальные проблемы правоприменительной практики в сфере образования.

Решение кейсов[*]

1. Большой юридический словарь определяет антикоррупционную политику следующим образом: это научно обоснованная, последовательная и системная деятельность институтов государства и гражданского общества, связанная с профилактикой и сокращением негативного влияния коррупции, а также с устранением причин и условий, способствующих ее возникновению. Ее принципами являются: научность; оперативность; последовательность и постепенность; недопустимость установления двойных стандартов; сочетание ограничительных и стимулирующих правовых средств; тесное сотрудничество международных организаций, институтов гражданского общества и государства; комплексное использование научных (всестороннее исследование коррупции, выявление слабых, уязвимых мест, разработка системы противодействия коррупции), организационных (создание раз-

[*] Кейсы взяты из открытых интернет-источников.

личных структур и их действия по борьбе с коррупцией), правовых (в первую очередь правотворческих – разработка и принятие следующих законов: «О противодействии коррупции», «О правовом регулировании лоббистской деятельности», «О борьбе с организованной преступностью») и иных мер. Поясните, насколько полно, на ваш взгляд, данное определение характеризует содержание антикоррупционной политики, осуществляемой в настоящее время в нашем государстве.

2. Как известно, в период правления российской императрицы Елизаветы Петровны канцлер Бестужев-Рюмин получал за службу Российской империи 7 тыс. руб. в год, а за услуги, оказываемые Британской короне (в качестве «агента влияния»), – 12 тыс. руб. Прокомментируйте данный исторический факт.

3. Как неоднократно подчеркивал С. Ю. Глазьев, коррупция и невежество – две стороны одной медали. Охарактеризуйте эту связь, если согласны (не согласны) с этим мнением.

4. Согласно исследованию, проведенному Институтом социологии Российской академии наук (2007), причины коррупции заключаются: в жадности и аморальности чиновников и бизнесменов – 70,1 %; неэффективности государства и несовершенстве законов – 63,3 %; низком уровне правовой культуры, а также правовом нигилизме значительного количества населения – 37,2 %; клановости и семейственности в системе государственной службы – 33,9 %; правовой неграмотности государственных служащих – 13,7 %; затруднились ответить – 4,2 %; назвали иные причины – 1,1 %. Явным злом коррупцию считают 2,5 % граждан. Чем объяснить последний показатель? Какие причины недостаточно полно учитываются реализуемой в настоящее время государственной политикой в сфере противодействия коррупции?

Методические рекомендации

В тетрадях для справочных материалов составьте ответы по плану кейсов в виде схем, таблиц, развернутых планов.

Тема 9. Уголовно-правовая характеристика коррупционных преступлений в образовании. Специфика организации АТЗ в образовательной организации.

План

1. Виды коррупционных правонарушений.
2. Уголовно-правовая характеристика коррупционной преступности.
3. Детерминанты коррупционной преступности.
4. Гражданско-правовые коррупционные деликты – обладающие признаками коррупции нарушения правил дарения, а также нарушения порядка предоставления услуг, предусмотренных законодательством РФ.
5. Дисциплинарные коррупционные проступки – обладающие признаками коррупции и не являющиеся преступлениями или административными правонарушениями проступки, за совершение которых законодательством Российской Федерации предусмотрена дисциплинарная ответственность.
6. Административные коррупционные правонарушения – обладающие признаками коррупции и не являющиеся преступлениями правонарушения, за совершение которых российским законодательством предусмотрена административная ответственность.
7. Субъективная сторона коррупционных преступлений, характеризующаяся умышленной виной (прямой или косвенный умысел).
8. Документы, регламентирующие АТЗ общеобразовательных учреждений.
9. Документы, регламентирующие АТЗ в высшей школе.
10. Проект памятки по АТЗ для общеобразовательных учреждений (инфографика).
11. Проект памятки по АТЗ для высшей школы (инфографика).
12. Мероприятия, направленные на организацию АТЗ в рамках административно-воспитательной работы.

Методические рекомендации

В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

7. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

7.1. Текущий контроль успеваемости

Рейтинг-контроль № 1

Тест

1. Право образовательного учреждения на выдачу своим выпускникам документа государственного образца о соответствующем уровне образования возникает:

а) с момента его государственной аккредитации;

б) лицензирования;

в) регистрации;

г) аттестации.

2. Граждане Российской Федерации имеют право на получение ___ образования на родном языке:

а) основного общего;

б) среднего (полного) общего;

в) начального;

г) высшего профессионального.

3. Законодательство Российской Федерации в области образования не включает в себя:

а) Декларацию принципов толерантности;

б) Конституцию Российской Федерации;

в) закон Российской Федерации «Об образовании»;

г) нормативные правовые акты субъектов Российской Федерации в области образования.

4. Государственный образовательный стандарт в условиях современной системы образования по закону Российской Федерации «Об образовании»:

а) является основой объективной оценки уровня образования и квалификации выпускников независимо от формы получения образования;

б) гарантирует получение бесплатного общего и на конкурсной основе бесплатного профессионального образования в государственных и муниципальных образовательных учреждениях;

в) обеспечивает качество подготовки специалистов;

г) обеспечивает право на равноценное образование.

5. В соответствии с законом «Об образовании» Российской Федерации формой получения образования не является:

а) непрерывное образование;

б) семейное образование;

в) самообразование;

г) экстернат.

6. Дополнительное образование в соответствии с законом Российской Федерации «Об образовании» предполагает:

а) всестороннее удовлетворение образовательных потребностей граждан и обеспечение непрерывного повышения квалификации;

б) реализацию содержания соответствующих программ в системе детских юношеских спортивных школ;

в) подготовку детей в домах творчества;

г) углубленное освоение образовательных программ.

7. Образование, цель которого – подготовка работников квалифицированного труда по всем основным направлениям общественно-полезной деятельности на базе основного общего образования, является:

а) начальным профессиональным образованием;

б) средним профессиональным;

в) высшим профессиональным;

г) дополнительным.

8. У образовательного учреждения возникает право на образовательную деятельность с момента:

а) выдачи лицензии;

б) регистрации;

в) государственной аккредитации;

г) уплаты налогов;

9. К ведущим принципам разработки содержания непрерывного педагогического образования не относится:

а) наглядность;

б) фундаментальность;

в) преемственность;

г) вариативность.

10. Общее руководство государственным или муниципальным высшим учебным заведением осуществляет:

а) ученый совет;

б) педагогический;

в) попечительский;

г) ректорский.

Рейтинг-контроль № 2

Тест

1. Соответствующий нормативным критериям уровень квалификации, профессионализма, позволяющий работнику решать задачи определенной степени сложности, – это:

а) квалификационная категория;

б) компетентность;

в) мастерство;

г) творчество.

2. Для аттестации педагогических работников на вторую квалификационную категорию аттестационная комиссия создается:

а) образовательным учреждением;

б) местным органом управления образованием;

в) попечительским советом;

г) федеральным органом управления образованием;

3. Документ, являющийся основой для определения нормативных критериев профессионально-педагогического уровня аттестуемого учителя:

а) квалификационная характеристика;

б) удостоверение о присвоении квалификационной категории;

в) единая тарифная сетка по оплате труда работников бюджетной сферы;

г) квалификационный разряд.

4. Одним из принципов аттестации педагогических и руководящих работников государственных и муниципальных образовательных учреждений является:

а) добровольность на вторую, первую и высшую квалификационные категории – для педагогических работников и на высшую квалификационную категорию – для руководящих работников;

б) добровольность для руководящих работников и лиц, претендующих на руководящую должность, на первую квалификационную категорию;

в) закрытость процесса обсуждения результатов;

г) обязательность аттестации на вторую, первую и высшую квалификационные категории для педагогических работников.

5. Квалификационные категории педагогическим и руководящим работникам присваивают сроком:

а) на 5 лет;

б) 1 год;

в) 3 года;

г) 10 лет.

6. При принятии решения по итогам аттестации учитель (руководитель) имеет право:

а) лично присутствовать;

б) участвовать в дискуссии;

в) проходить повторную аттестацию в ближайшее время;

г) участвовать в голосовании;

7. Тарифно-квалификационные характеристики по должностям работников учреждений и организаций образования служат основой:

а) при проведении аттестации;

б) написании характеристики учителя;

в) повышении квалификации;

г) планировании педагогической деятельности.

8. Количество категорий, установленных в соответствии с квалификационными требованиями, составляет:

а) 3;

б) 7;

в) 9;

г) 14.

9. Аттестуемый педагогический или руководящий работник вправе избрать:

а) конкретные формы и процедуры аттестации из числа вариативных форм и процедур;

б) сроки прохождения аттестации;

в) состав аттестационной комиссии;

г) срок действия установленной аттестационной категории.

10. Документ, регулирующий деятельность общеобразовательных учреждений и являющийся основой для разработки учреждением устава:

а) Типовое положение об общеобразовательном учреждении;

б) закон Российской Федерации «Об образовании»;

в) Положение о порядке аттестации педагогических и руководящих работников государственных и муниципальных образовательных учреждений;

г) Федеральная целевая программа развития образования.

Рейтинг-контроль № 3

Тест

1. К приоритетным задачам модернизации российского образования не относится:

а) усиление государственного контроля за качеством образования;

б) обеспечение государственных гарантий доступности и равных возможностей получения полноценного образования;

в) достижение нового современного качества дошкольного, общего и профессионального образования;

г) формирование в системе образования нормативно-правовых и организационно-экономических механизмов привлечения и использования внебюджетных ресурсов.

2. Документ, защищающий права ребенка и имеющий обязательную силу для подписавших его стран:

а) конвенция;

б) декларация;

в) программа;

г) концепция.

3. Конвенция ООН о правах ребенка была ратифицирована в России:

а) в 1990 году;

б) 1994 году;

в) 1989 году;

г) 1918 году.

4. Ребенком является лицо в возрасте:

а) до 18 лет;

б) 16 лет;

в) 14 лет;

г) 12 лет.

5. Является ли верным суждение: «Коррупциогенный фактор – это положение нормативного правового акта (проекта нормативного правового акта), устанавливающее для правоприменителя необоснованно широкие пределы усмотрения или возможность необоснованного применения исключений из общих правил, а также положение, содержащее неопределенные, трудновыполнимые и (или) обременительные требования к гражданам и организациям и тем самым создающее условия для проявления коррупции.

6. Какая ответственность предусмотрена за привлечение работодателем либо заказчиком работ (услуг) к трудовой деятельности на условиях трудового договора либо к выполнению работ или оказанию услуг на условиях гражданско-правового договора гражданского служащего, замещающего должность, включенную в перечень, установленный нормативными правовыми актами, либо бывшего гражданского служащего, замещавшего такую должность, с нарушением требований, предусмотренных федеральным законом «О противодействии коррупции»?

7. Может ли государственный гражданский служащий принимать награды, почетные и специальные звания иностранных государств, международных организаций, а также политических партий, других общественных объединений и религиозных объединений, если в его должностные обязанности входит взаимодействие с указанными организациями и объединениями?

8. В какой форме обязан уведомить гражданский служащий о возникшем конфликте интересов или о возможности его возникновения?

9. Кого обязан уведомить гражданский служащий о возникшем конфликте интересов или о возможности его возникновения?

10. Является ли основанием для отказа в приёме гражданина на государственную (муниципальную) службу непредставление гражданином при поступлении на государственную (муниципальную) службу сведений о своих доходах, имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера своих супруги (супруга) и несовершеннолетних детей либо представление заведомо недостоверных или неполных сведений?

11. Какие, на ваш взгляд, меры совершенствования информационно-пропагандистского характера и защиты информационного пространства Российской Федерации от идеологии терроризма эффективны?

12. Согласно какому документу одним из основных направлений государственной национальной политики Российской Федерации является противодействие пропаганде идей экстремизма в средствах массовой информации и электронных коммуникаций?

13. Какие существуют факторы формирования угрозы для национальной безопасности в киберсреде?

14. Какие виды силового давления на государство существуют в настоящее время?

15. Какая из перечисленных стран блокирует доступ населения ко многим международным социальным сетям с целью минимизации угроз для своей безопасности?

а) Российская Федерация;

б) КНР;

в) США.

16. Какие платформы в Интернете использовались для пропаганды терроризма?

17. Какие направления может включать в себя контрпропагандистская деятельность в сфере противодействия терроризму?

18. Что создается для профилактики террористической деятельности на сайтах университетов?

19. Какое явление способствует диджитализации пропагандистской деятельности в Интернете?

20. Как современный университет может противодействовать пропаганде терроризма и его киберформы?

7.2. Промежуточная аттестация

По итогам освоения дисциплины проводится *зачет.*

Контрольные вопросы к зачету

1. Академические свободы вуза при реализации основных образовательных программ высшего профессионального образования.
2. Государственно-общественные и общественные организации в сфере образования.
3. Государственный образовательный стандарт общего образования как нормативный документ, регламентирующий работу образовательной организации.
4. Законодательство Российской Федерации как инструмент защиты прав ребенка.
5. Источники законодательства об образовании.
6. Источники финансирования образовательных учреждений.
7. Классификация образовательных учреждений по их организационно-правовой форме.
8. Конвенция о правах ребенка и ее основные положения.
9. Конституция Российской Федерации как основа правового регулирования сферы образования.
10. Материальные и правовые гарантии на образование.
11. Многоуровневые образовательные модели.
12. Назначение и структура государственных образовательных стандартов.
13. Непрерывность и преемственность образовательных программ различного уровня.
14. Нормативно-правовое обеспечение высшего и послевузовского образования.
15. Нормативно-правовое обеспечение дошкольного образования.
16. Нормативно-правовое обеспечение начального и среднего профессионального образования.
17. Нормативно-правовое обеспечение школьного образования.

18. Нормативно-правовые документы, регламентирующие деятельность образовательных организаций. Формы получения образования.

19. Образовательные организации высшего профессионального образования, их задачи и структура. Автономия образовательных организаций высшего профессионального образования и академические свободы.

20. Образовательные правоотношения.

21. Общая характеристика законодательства об образовании.

22. Общая характеристика зарубежных образовательных систем.

23. Общая характеристика международных правовых актов.

24. Общие требования к содержанию образования.

25. Организационная структура государственно-общественной системы аттестации и контроля качества образования.

26. Основные законодательные акты в сфере образования.

27. Основные направления модернизации российской системы образования.

28. Основные недостатки и противоречия действующего образовательного законодательства.

29. Основные положения закона Российской Федерации «Об основных гарантиях прав ребенка в Российской Федерации».

30. Основные положения Конвенции о правах ребенка.

31. Основные права ребенка и формы их правовой защиты в законодательстве Российской Федерации.

32. Основные структурные элементы системы образования.

33. Основные характеристики образовательного процесса.

34. Основные элементы системы образования и их взаимодействие. Интеграционные процессы в области образования.

35. Особенности правового регулирования трудовых отношений в сфере образования.

36. Платность дополнительных образовательных услуг в государственных и муниципальных учреждениях.

37. Подход к оценке качества подготовки по различным образовательным программам.

38. Понятие образовательной услуги.

39. Послевузовское и дополнительное профессиональное образование.

40. Права и обязанности учащихся образовательных учреждений.

41. Права и обязанности, ответственность образовательных учреждений перед личностью, обществом и государством.

42. Право на образование: проблемы его реализации.

43. Правовая регламентация приема в образовательное учреждение.

44. Правовой статус образовательного учреждения и образовательной организации.

45. Правовые основы создания информационно-аналитического обеспечения образования.

46. Принципы государственной образовательной политики. Политика децентрализации управления системой образования.

47. Принципы государственной политики в области образования. Роль государства в становлении и развитии системы образования.

48. Принципы государственной политики в сфере образования.

49. Программа модернизации педагогического образования.

50. Роль государства в сфере образования.

51. Роль государственных, государственно-общественных и общественных структур управления в сфере образования.

52. Система государственного контроля обеспечения образования.

53. Системы аккредитации зарубежных стран. Система аккредитации США: институциональная и специализированная. Цели, содержание системы оценки качества образования в США. Особенности общественной аккредитации образовательных учреждений России.

54. Смежные законодательные акты, затрагивающие область образования.

55. Сотрудничество образовательных учреждений с органами правопорядка и социальной защиты населения.

56. Специфика образовательных отношений. Понятие образовательного права.

57. Структура высшего профессионального образования.

58. Структура нормативно-правового и научно-методического обеспечения сферы образования.

59. Структура системы государственного контроля в сфере образования. Лицензирование, аттестация, аккредитация.

60. Субъекты образовательного права.

61. Типовые положения и устав образовательных учреждений и организаций.

62. Типы и виды образовательных программ.

63. Типы и виды образовательных учреждений. Автономия образовательных учреждений.

64. Типы образовательных организаций. Порядок их создания, реорганизации и ликвидации.

65. Управление системой образования.

66. Управление учебным процессом на уровне образовательного учреждения.

67. Условия реализации государственных образовательных стандартов общего и высшего профессионального образования.

68. Формирование системы дополнительного общего и профессионального образования. Правовое и нормативное обеспечение дополнительного образования. Рабочая программа дисциплины «Нормативно-правовое обеспечение профессиональной деятельности».

69. Формирование структуры и содержание образования.

70. Функции государственных и муниципальных органов управления образованием.

71. Цели, содержание, порядок лицензирования и аккредитации образовательных организаций. Различие между российской и зарубежными системами аккредитации образовательных организаций.

72. Конвенция ООН (межконтинентальная) против коррупции, принятая Генеральной Ассамблеей ООН 31 октября 2003 года: содержание, назначение.

73. Конвенция Совета Европы (континентальная) о борьбе с коррупцией от 6 ноября 1998 года: основные положение, назначение.

74. Активный и пассивный подкуп в частном секторе как деяние коррупционного характера (согласно Конвенции Совета Европы о борьбе с коррупцией от 6 ноября 1998 года).

75. Роль федерального закона от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции» в определении стратегии борьбы с обозначенным противоправным явлением.

76. Понятие коррупции по законодательству Российской Федерации.

77. Основные принципы противодействия коррупции правоохранительными органами Российской Федерации.

78. Организационные основы противодействия коррупции в Российской Федерации.

79. Основные статистические данные, характеризующие коррупцию.

80. Уголовно-правовая характеристика коррупционных преступлений.

81. Понятие и виды коррупционных преступлений согласно законодательству Российской Федерации.

82. Уголовно-правовая характеристика коррупционной преступности и основные направления ее предупреждения.

83. Криминологическая характеристика коррупционной преступности.

84. Основные данные, составляющие типичный портрет коррупционера в Российской Федерации.

85. Правовые основы предотвращения и урегулирования конфликта интересов на государственной службе.

86. Особенности правового положения государственного служащего и антикоррупционные требования к его служебному поведению.

87. Понятие, сущность, характерные черты и тенденции современного терроризма. Терроризм как опасное социально-политическое явление.

88. Понятие, сущность, характерные черты и тенденции современного экстремизма. Экстремизм как опасное социально-политическое явление.

89. Отличительные признаки терроризма. Причины и условия возникновения и распространения терроризма.

90. Отличительные признаки экстремизма. Причины и условия возникновения и распространения экстремизма.

91. Основные подходы в понимании методов борьбы с терроризмом на современном этапе. Основные тенденции современного терроризма.

92. Терроризм как угроза национальной безопасности Российской Федерации.

93. Концепция противодействия терроризму в Российской Федерации.

94. Основные внутренние факторы, обусловливающие возникновение и распространение терроризма и экстремизма в Российской Федерации.

95. Основные внешние факторы, обусловливающие возникновение и распространение терроризма и экстремизма в Российской Федерации.

96. Объекты террористических устремлений в Российской Федерации.

97. Полномочия федеральных органов исполнительной власти в формировании и реализации основных направлений государственной политики Российской Федерации в области противодействия терроризму.

98. Участие федеральных органов исполнительной власти в государственной политике Российской Федерации в области информационного противодействия терроризму.

99. Организационные и правовые основы противодействия терроризму в России.

100. О комплексе мероприятий, направленных на достижение цели и задач Комплексного плана противодействия идеологии терроризма в Российской Федерации на 2019 – 2023 годы.

101. Координация и контроль деятельности по исполнению Комплексного плана.

102. Финансовое обеспечение деятельности по исполнению Комплексного плана.

103. Роль Национального антитеррористического комитета (НАК) как органа, обеспечивающего координацию деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления по противодействию терроризму.

104. Основные задачи и направления деятельности Национального антитеррористического комитета.

105. О координирующей роли антитеррористических комиссий по вопросам противодействия терроризму в субъектах Российской Федерации.

106. Функции должностных лиц органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления, на которые возложено непосредственное руководство работой по исполнению мероприятий Комплексного плана. Цели и задачи их деятельности.

107. Отражение мероприятий Комплексного плана противодействия идеологии терроризма в Российской Федерации в различных документах органов исполнительной власти субъектов Российской Федерации.

108. Разработка региональных планов (программ) в сфере противодействия идеологии терроризма.

109. Особенности функционирования экспертных советов для выработки информационной политики в сфере профилактики терроризма (планирование работы, заседания, проведение конкретных мероприятий, отчеты).

110. Организация работы по информационному противодействию терроризму.

111. Вопросы взаимодействия между различными организациями в целях эффективного исполнения мероприятий Комплексного плана противодействия идеологии терроризма в Российской Федерации.

7.3. Самостоятельная работа обучающегося

Тема 1. Актуальные правовые проблемы в сфере образовательных отношений в Российской Федерации.

1. Обобщите изученные по теме материалы в виде схем, таблиц, развернутых планов, моделей.

2. Составьте библиографический список литературы по теме, включив в него имеющиеся в библиотеке монографии, сборники, статьи одного из периодических изданий за последние пять лет.

3. В тетрадях для практических занятий решите проблемные ситуации. Выберите правильный ответ и подтвердите его соответствующей статьей федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации».

Задание 1. Кто несет ответственность за качество образования выпускников? а) образовательная организация; б) учитель; в) руководитель образовательной организации; г) руководитель, учителя, родители (законные представители) обучающихся образовательной организации.

Задание 2. Могут ли быть созданы и осуществлять свою деятельность в образовательной организации общественные объединения обучающихся, в том числе профессиональный союз? а) профсоюз – да, общественные объединения обучающихся – нет; б) профсоюз – нет; общественные объединения обучающихся – да; в) да; г) нет.

Задание 3. Если учитель решил применять в своей деятельности новую методику, предусматривающую практические занятия, в ходе которых от обучающихся требуется выполнить определенные трудовые функции, то каким образом он должен обеспечить внедрение этой методики? а) включить практические занятия в свой рабочий план и потребовать от обучающихся обязательного выполнения предусмотренных этим планом трудовых функций; б) согласовать этот вопрос с заместителем директора и проводить эти практические занятия в обычном порядке; в) обратиться к руководителям образовательной организации с просьбой о включении этих занятий в образовательную программу и учебный план и после включения приступить к этим занятиям; г) проведение занятий, требующих от обучающихся выполнения определенных трудовых функций, не допускается.

4. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 2. Организация противодействия идеологии терроризма в Российской Федерации (в соответствии с Комплексным планом противодействия идеологии терроризма в Российской Федерации).

1. Обобщите изученные по теме материалы в виде схем, таблиц, развернутых планов, моделей.

2. Составьте библиографический список литературы по теме, включив в него имеющиеся в библиотеке монографии, сборники, статьи одного из периодических изданий за последние пять лет.

3. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 3. Государственная политика в области образования, ее правовая регламентация. Меры по формированию у молодежи антитеррористического сознания и информационно-коммуникативной культуры.

1. Обобщите изученные по теме материалы в виде схем, таблиц, развернутых планов, моделей.

2. Составьте библиографический список литературы по теме, включив в него имеющиеся в библиотеке монографии, сборники, статьи одного из периодических изданий за последние пять лет.

3. В тетрадях для практических занятий решите проблемные ситуации. Выберите правильный ответ и подтвердите его соответствующей статьей федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации».

Задание 1. Что в соответствии с законом Российской Федерации «Об образовании в Российской Федерации» является основой объективной оценки подготовки выпускников, освоивших основные образовательные программы? а) государственная аттестация выпускников, проводимая независимой от органов управления образования государственной аттестационно-диагностической службой; б) федеральные государственные образовательные стандарты; в) общественно-государственный контроль деятельности образовательных организа-

ций; г) основа объективной оценки подготовки выпускников в законе не определена.

Задание 2. Примерная основная образовательная программа – это: а) примерный учебный план; б) примерный календарный учебный график; в) примерные рабочие программы учебных предметов, курсов, дисциплин и иных компонентов; г) учебно-методическая документация, включающая все вышеназванные компоненты: а) б) в).

Задание 3. Какое решение директора школы следует считать правильным, с точки зрения закона, по поводу выпускника 9-го класса, имевшего отличную успеваемость по математике на протяжении всей учебы, но отказавшегося сдавать по предмету выпускной экзамен? а) выдать вместо аттестата справку об обучении установленного образца; б) всеми возможными и невозможными способами заставить его явиться на экзамен, так как итоговая аттестация после окончания основной школы обязательна; в) аттестовать с учетом оценок промежуточных аттестаций и неявки на экзамен; г) ничего не предпринимать, возложив ответственность на родителей (законных представителей) выпускника

4. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 4. Создание позитивного контента в системе противодействия распространению идеологии терроризма, экстремизма в киберсреде. Практика разработки профилактических психолого-педагогических методических материалов по противодействию экстремизму и терроризму в молодежной среде.

1. Обобщите изученные по теме материалы в виде схем, таблиц, развернутых планов, моделей.

2. Составьте библиографический список литературы по теме, включив в него имеющиеся в библиотеке монографии, сборники, статьи одного из периодических изданий за последние пять лет.

3. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 5. Нормативно-правовые и организационные основы деятельности образовательных учреждений.

1. Обобщите изученные по теме материалы в виде схем, таблиц, развернутых планов, моделей.

2. Составьте библиографический список литературы по теме, включив в него имеющиеся в библиотеке монографии, сборники, статьи одного из периодических изданий за последние пять лет.

3. В тетрадях для практических занятий решите проблемные ситуации. Выберите правильный ответ и подтвердите его соответствующей статьей федерального закона от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации».

Задание 1. На какой срок в соответствии с законом выдается лицензия на образовательную деятельность? а) бессрочно; б) на три года; в) на пять лет; г) срок законом не установлен.

Задание 2. Если учителю при приеме на работу дали ознакомиться с тремя образовательными программами (рекомендованной Минобразованием РФ; инновационной, опубликованной в сети Интернет; утвержденной образовательной организацией), то какую из них он должен считать обязательной основой для своей деятельности? а) программу, рекомендованную Минобразованием РФ; б) инновационную программу, опубликованную в сети Интернет; в) программу, утвержденную образовательным учреждением; г) любую из перечисленных программ по своему выбору.

Задание 3. В чью компетенцию входит научно-методическое обеспечение системы образования? а) федеральных органов исполнительной власти, осуществляющих государственное управление в сфере образования; б) органов исполнительной власти субъектов Российской Федерации, осуществляющих государственное управление в сфере образования; в) федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации, осуществляющих государственное управление в сфере образования; г) федеральных органов управления образованием.

4. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 6. Образовательные стандарты: виды, сравнение, отличия.

1. Обобщите изученные по теме материалы в виде схем, таблиц, развернутых планов, моделей.

2. Составьте библиографический список литературы по теме, включив в него имеющиеся в библиотеке монографии, сборники, статьи одного из периодических изданий за последние пять лет.

3. В тетрадях для практических занятий решите проблемные ситуации.

Задание 1. Какой продолжительности рабочая неделя определена в федеральном законе от 29 декабря 2012 года № 273-ФЗ «Об образовании в Российской Федерации» для учителя общеобразовательной школы? а) 40 часов; б) не более 36 часов; в) 18 часов; г) длительность рабочей недели для педагогических работников определена как сокращенная продолжительность рабочего времени.

Задание 2. Может ли образовательная организация без ведома учредителя изменить порядок проведения промежуточной аттестации и используемую при этом систему оценок? а) да, это компетенция образовательного учреждения; б) да, но только порядок проведения промежуточной аттестации; в) да, но только систему оценок, используемую при проведении промежуточной, точной аттестации; г) нет.

Задание 3. Как следует поступить учителю, если обучающийся только по его предмету имеет академическую задолженность по итогам года, а учитель не считает, что нет необходимости оставлять этого ученика на второй год? а) самостоятельно исправить оценку на положительную и рекомендовать органам управления образовательной организацией перевести обучающегося в следующий класс на общих основаниях; б) постараться договориться с администрацией образовательной организации и с ее разрешения исправить оценку на положительную; в) поставить вопрос об осенней переэкзаменовке обучающегося; г) ходатайствовать перед органом управления образовательной организации об условном переводе этого ученика в следующий класс.

4. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 7. Образовательное право России в мировом образовательном пространстве: актуальные проблемы развития.

1. Обобщите изученные по теме материалы в виде схем, таблиц, развернутых планов, моделей.

2. В тетрадях для практических занятий решите проблемные ситуации.

Задание 1. Вправе ли муниципальная или государственная аккредитованная образовательная организация самостоятельно устанавливать нормативные сроки освоения основных образовательных программ? а) да, безусловно; б) да, но только с согласия учредителя; в) да, при условии соблюдения требования о максимальной нагрузке, устанавливаемой стандартом; г) нет.

Задание 2. Законно ли требование учителя об отчислении из муниципальной школы ученика 7-го класса, достигшего возраста 13 лет, за то, что тот «ленится и совершенно не желает изучать его предмет»? а) да, такое требование вполне правомерно, и администрация школы, не нарушая требований закона, может его удовлетворить; б) да, требование правомерно, но только в случае, если этот ученик к тому же неоднократно нарушил устав образовательного учреждения и (или) совершил противоправные действия; в) да, правомерно, если аналогичные требования поступают и от других учителей; г) нет.

Задание 3. Какую систему оценок следует использовать при промежуточной аттестации обучающихся? а) общепринятую в России четырехбалльную систему; б) систему, произвольно выбранную учителем, для текущего контроля знаний обучающихся; в) любую систему, установленную на данный период Советом образовательной организации; г) систему, установленную образовательной организацией.

3. В тетрадях для справочных материалов составьте ответы по плану практического занятия в виде схем, таблиц, развернутых планов.

Тема 8. Законодательные акты Российской Федерации по противодействию коррупции: актуальные проблемы правоприменительной практики в сфере образования.

Составьте смысловые карты на основе приведенных утверждений (в виде схем, рисунков, моделей):

1. Понятие коррупции и система уголовно-правовых средств борьбы с этим явлением.

2. Коррупция как фактор организованной преступности в сфере экономики.

3. Коррупция в государственном механизме современной России: теоретические аспекты.

4. Коррупция и международное сотрудничество в борьбе с ней.

5. Коррупция как общеправовой феномен.

6. Коррупция в органах государственной власти: теория, практика и механизмы антикоррупционной политики.

7. Коррупция в системе государственной службы в России: истоки и тенденции.

8. Коррупционная преступность в органах внутренних дел.

9. Коррупция как социальное и экономическое явление.

10. Коррупция в российском избирательном процессе: понятие и противодействие.

11. Коррупция в образовательном секторе.

Тема 9. Уголовно-правовая характеристика коррупционных преступлений в образовании. Специфика организации АТЗ в образовательной организации.

Составьте смысловые карты на основе приведенных утверждений (в виде схем, рисунков, моделей):

1. Коррупция как угроза экономической безопасности России.

2. Административно-правовые средства предупреждения и пресечения коррупции в системе государственной службы Российской Федерации.

3. Коррупция как фактор угрозы национальной безопасности Российской Федерации.

4. Политическая коррупция как форма теневой власти.

5. Коррупция в органах государственной власти Российской Федерации.

6. Понятие коррупции (криминологический аспект) и меры ее предупреждения в государственном аппарате.

7. Противодействие коррупции: соотношение международно-правового и внутригосударственного регулирования.

8. Противодействие коррупционной преступности в России: ретроспектива, современность и перспективы.

9. Коррупция в Российской Федерации: сущность, особенности и основные направления противодействия.

10. Рекомендации по АТЗ для образовательной организации.

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Книгообеспеченность

Автор, название, вид издания, издательство	Год издания	Книгообеспеченность / наличие в электронном каталоге ЭБС
Основная литература		
Юдина, А. М. Современные подходы к исследованию информационно-коммуникативной культуры студентов : монография / Л. К. Фортова, А. М. Юдина ; Мин-во образования и науки Рос. Федерации, ФБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых». – Владимир : Шерлок-пресс, 2021. – 80 с. – ISBN 978-5-907197-60-2	2020	5 шт.
Менеджмент в системе образования : хрестоматия / О. Г. Ерофеева [и др.] ; под ред. канд. пед. наук О. Г. Ерофеевой ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2020. – 252 с. – ISBN 978-5-9984-0955-4	2020	https://dspace.www1.vlsu.ru/bitstream/123456789/8316/3/01944.pdf
Смаковская, Н. И. Нормативно-правовое обеспечение профессиональной деятельности : учеб. пособие / Н. И. Смаковская ; Влад. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2021 – 163 с. – ISBN 978-5-9984-1383-4	2021	https://dspace.www1.vlsu.ru/bitstream/123456789/8926/1/02150.pdf
Дополнительная литература		
Юдакова, С. В. Психолого-педагогические аспекты менеджмента в сфере образования : учеб. пособие / С. В. Юдакова ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2020. – 111 с. – ISBN 978-5-9984-1134-2	2020	https://dspace.www1.vlsu.ru/bitstream/123456789/8312/1/01940.pdf
Сергеев, А. Г. Качество высшего образования : учеб. пособие / А. Г. Сергеев, В. В. Кучерова, В. М. Баландин ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. – Владимир : Изд-во ВлГУ, 2017. – 83 с. – ISBN 978-5-9984-0765-9	2017	https://dspace.www1.vlsu.ru/bitstream/123456789/5907/1/01619.pdf
Методические рекомендации по организации профилактической работы в образовательных организациях высшего образования, реализуемой в рамках учебного процесса, а также общевоспитательных, патриотических и досуговых мероприятий / под общ. ред. С. А. Чурилова. – М. ; Ростов н/Д., 2022. – 30 с.	2022	https://morflot.gov.ru/media/ffbpswvi/metodika.pdf

8.2. Периодические издания

1. Журнал «Народное образование» (рус.). – научный электронный журнал, включен в Перечень ВАК. URL: http://narodnoe.org/

2. Журнал «Образование и право» (рус.) – научно-правовой электронный журнал, включен в перечень ВАК. URL: https://education.law-books.ru/

8.3. Интернет-ресурсы

1. Конституция Российской Федерации (принята всенародным голосованием 12 дек.1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.). URL: https://www. consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 14.04.2023).

2. Федеральный закон от 29 дек. 2012 г. № 273-ФЗ «Об образовании в Российской Федерации». URL: https://www.consultant.ru/ document/cons_doc_LAW_140174/ (дата обращения: 14.04.2023).

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 14.04.2023).

4. Федеральный закон от 30 дек. 2020 г. № 489-ФЗ «О молодежной политике в Российской Федерации». URL: https://www. consultant.ru/document/cons_doc_LAW_372649/ (дата обращения: 14.04.2023).

5. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности». URL: https://www. consultant.ru/document/cons_doc_LAW_37867/ (дата обращения: 14.04.2023).

6. Федеральный закон от 23 июня 2016 г. № ФЗ-182 «Об основах системы профилактики правонарушений». URL: https://www. consultant.ru/document/cons_doc_LAW_199976/ (дата обращения: 14.04.2023).

7. Федеральный закон от 6 марта 2006 г. № ФЗ-35 «О противодействии терроризму». URL: https://www.consultant.ru/document/ cons_doc_LAW_58840/ (дата обращения: 14.04.2023).

8. Концепция противодействия терроризму в Российской Федерации, утвержденная Президентом Российской Федерации 5 окт. 2009 г. URL: https://www.consultant.ru/document/cons_doc_LAW_92779/ (дата обращения: 14.04.2023).

9. Комплексный план противодействия идеологии терроризма в Российской Федерации на 2019 – 2023 годы (утвержден Президентом Российской Федерации 28 дек. 2018 г. № Пр-2665). URL: https://www.consultant.ru/document/cons_doc_LAW_402397/ (дата обращения: 14.04.2023).

10. Указ Президента Российской Федерации от 29 мая 2020 г. № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года». URL: https://www. consultant.ru/document/cons_doc_LAW_353838/ (дата обращения: 14.04.2023).

11. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» (утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400). URL: https://www.consultant.ru/document/ cons_doc_LAW_162169/ (дата обращения: 14.04.2023).

12. Указ Президента Российской Федерации от 9 нояб. 2022 № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей». URL: https://www.consultant.ru/document/cons_doc_LAW_430906/ (дата обращения: 14.04.2023).

13. Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам». URL: https://www.consultant.ru/ document/cons_doc_LAW_151143/ (дата обращения: 14.04.2023).

14. Приказ Министерства труда и социальной защиты Российской Федерации от 10 марта 2021 г. № 116н «Об утверждении профессионального стандарта “Руководитель образовательной организации высшего образования”». URL: https://www.consultant.ru/document/ cons_doc_LAW_382174/ (дата обращения: 14.04.2023).

15. Приказ Минтруда России от 12 февр. 2020 № 59н «Об утверждении профессионального стандарта “Специалист по работе с молодежью”». URL: https://www.consultant.ru/document/cons_doc_LAW_ 354196/ (дата обращения: 14.04.2023).

16. Приказ Минтруда России от 2 авг. 2018 г. № 514н «Об утверждении профессионального стандарта “Специалист в сфере национальных и религиозных отношений” (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 2 августа 2018 г. № 514н).

URL: https://www.consultant.ru/document/cons_doc_LAW_306412/ (дата обращения: 14.04.2023).

17. Приказ Минтруда России от 12 апр. 2013 г. № 148н «Об утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов». URL: https://www.consultant.ru/document/cons_doc_LAW_146970/ (дата обращения: 14.04.2023).

18. Приказ Минобрнауки России от 13 авг. 2020 № 1016 (ред. от 26 нояб. 2020 г.) «Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 38.03.04 Государственное и муниципальное управление». URL: https://www.consultant.ru/document/cons_doc_LAW_360855/ (дата обращения: 14.04.2023).

19. Постановление Правительства Российской Федерации от 22 янв. 2013 г. № 23 «О Правилах разработки, утверждения и применения профессиональных стандартов». URL: https://www.consultant.ru/document/cons_doc_LAW_141271/ (дата обращения: 14.04.2023).

20. Постановление Правительства РФ от 29 дек. 2016 № 1532 (ред. от 9 дек. 2022 г.) «Об утверждении государственной программы Российской Федерации «Реализация государственной национальной политики» (с изм. и доп., вступ. в силу с 1 янв. 2023 г.). URL: https://www.consultant.ru/document/cons_doc_LAW_210753/ (дата обращения: 14.04.2023).

21. Постановление Правительства Российской Федерации от 4 мая 2008 г. № 333 «О компетенции федеральных органов исполнительной власти, руководство деятельностью которых осуществляет Правительство Российской Федерации, в области противодействия терроризму». URL: https://www.consultant.ru/document/cons_doc_LAW_76635/ (дата обращения: 14.04.2023).

22. Постановление Правительства Российской Федерации от 25 марта 2015 г. № 272 (ред. от 29.07.2020) «Об утверждении требований к антитеррористической защищенности мест массового пребывания людей и объектов (территорий), подлежащих обязательной охране войсками национальной гвардии Российской Федерации, и форм паспортов безопасности таких мест и объектов (территорий)». URL: https://www.consultant.ru/document/cons_doc_LAW_177496/ (дата обращения: 14.04.2023).

23. Постановление Правительства Российской Федерации от 22 дек. 2013 г. № 1244 (ред. от 5 марта 2022 г.) «Об антитеррористической защищенности объектов (территорий)» (вместе с «Правилами разработки требований к антитеррористической защищенности объектов (территорий) и паспорта безопасности объектов (территорий)»). URL: https://www.consultant.ru/document/cons_doc_LAW_156489/ (дата обращения: 14.04.2023).

24. Письмо Минобрнауки России от 12 марта 2015 г. № АК-610/06 «О направлении методических рекомендаций» (вместе с «Методическими рекомендациями по разработке, порядку выдачи и учету документов о квалификации в сфере дополнительного профессионального образования». URL: https://www.consultant.ru/document/cons_doc_LAW_177814/ (дата обращения: 14.04.2023).

25. Единый квалификационный справочник должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей работников учреждений органов по делам молодежи» (утверждён приказом Министерства здравоохранения и социального развития Российской Федерации от 28 нояб. 2008 г. № 678»). URL: https://www.consultant.ru/document/cons_doc_LAW_82742/ (дата обращения: 14.04.2023).

26. Пункт 3.17. «Вид профессиональной служебной деятельности. Регулирование в сфере противодействия терроризму» (в соответствии с Перечнем специальностей и направлений подготовки высшего образования, утвержденным приказом Минобрнауки России от 12 сент. 2013 г. № 1061), к специальностям, направлениям подготовки, знаниям и умениям, которые необходимы для замещения должностей государственной гражданской службы с учетом области и вида профессиональной служебной деятельности государственных гражданских служащих. URL: https://www.consultant.ru/document/cons_doc_LAW_153430/ (дата обращения: 14.04.2023).

27. Устав и другие локальные нормативные акты ВлГУ. URL: https://www.vlsu.ru/index.php?id=1099 (дата обращения: 14.04.2023).

28. ЭБС «Университетская библиотека ONLINE». URL: https://biblioclub.ru/

29. ЭБС «Консультант студента». URL: http://www.studentlibrary.ru/

30. ЭБС «IPRbooks». URL: http://www.iprbookshop.ru/

31. ЭБС «Znanium». URL: http://www. http://znanium.com/

32. ЭБС «БиблиоРоссика». URL: http://www.bibliorossica.com/

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации дисциплины имеются специальные помещения для проведения занятий лекционного типа, занятий практического типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы. Практические работы проводятся в аудиториях 7-го корпуса. Для обеспечения дисциплины имеется мультимедийное оборудование (проектор, экран, интерактивная доска).

Перечень используемого лицензионного программного обеспечения: операционная система семейства Microsoft Windows; пакет офисных программ Microsoft Office; Acrobat Reader; Google Chrome; 7-Zip; мультимедийные средства (ноутбук, проектор).

Приложение 2

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБ УТВЕРЖДЕНИИ ОСНОВ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО СОХРАНЕНИЮ И УКРЕПЛЕНИЮ ТРАДИЦИОННЫХ РОССИЙСКИХ ДУХОВНО-НРАВСТВЕННЫХ ЦЕННОСТЕЙ

В соответствии с Федеральным законом от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации» постановляю:

1. Утвердить прилагаемые Основы государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей.

2. Настоящий Указ вступает в силу со дня его подписания.

Президент
Российской Федерации
В. ПУТИН

Москва, Кремль
9 ноября 2022 года
№ 809

Утверждены
Указом Президента
Российской Федерации
от 9 ноября 2022 г. № 809

ОСНОВЫ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ПО СОХРАНЕНИЮ И УКРЕПЛЕНИЮ ТРАДИЦИОННЫХ РОССИЙСКИХ ДУХОВНО-НРАВСТВЕННЫХ ЦЕННОСТЕЙ

I. Общие положения

1. Настоящие Основы являются документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, определяющим систему целей, задач и инструментов реализации стратегического национального приоритета «Защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти» в части, касающейся защиты традиционных российских духовно-нравственных ценностей (далее также – традиционные ценности).

2. Нормативно-правовую базу настоящих Основ составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права и международные договоры Российской Федерации, Федеральный закон от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации», Основы государственной политики в сфере стратегического планирования в Российской Федерации.

3. Настоящие Основы конкретизируют отдельные положения Стратегии национальной безопасности Российской Федерации, Доктрины информационной безопасности Российской Федерации, Стратегии противодействия экстремизму в Российской Федерации до 2025 года, Стратегии государственной национальной политики Российской Федерации на период до 2025 года, Основ государственной культурной политики, Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы, указов Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до

2024 года» и от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года».

4. Традиционные ценности – это нравственные ориентиры, формирующие мировоззрение граждан России, передаваемые от поколения к поколению, лежащие в основе общероссийской гражданской идентичности и единого культурного пространства страны, укрепляющие гражданское единство, нашедшие свое уникальное, самобытное проявление в духовном, историческом и культурном развитии многонационального народа России.

5. К традиционным ценностям относятся **жизнь, достоинство, права и свободы человека, патриотизм, гражданственность, служение Отечеству и ответственность за его судьбу, высокие нравственные идеалы, крепкая семья, созидательный труд, приоритет духовного над материальным, гуманизм, милосердие, справедливость, коллективизм, взаимопомощь и взаимоуважение, историческая память и преемственность поколений, единство народов России.**

6. Христианство, ислам, буддизм, иудаизм и другие религии, являющиеся неотъемлемой частью российского исторического и духовного наследия, оказали значительное влияние на формирование традиционных ценностей, общих для верующих и неверующих граждан. Особая роль в становлении и укреплении традиционных ценностей принадлежит православию.

7. Российская Федерация рассматривает традиционные ценности как основу российского общества, позволяющую защищать и укреплять суверенитет России, обеспечивать единство нашей многонациональной и многоконфессиональной страны, осуществлять сбережение народа России и развитие человеческого потенциала.

8. Осмысление социальных, культурных, технологических процессов и явлений с опорой на традиционные ценности и накопленный культурно-исторический опыт позволяет народу России своевременно и эффективно реагировать на новые вызовы и угрозы, сохраняя общероссийскую гражданскую идентичность.

9. Государственная политика Российской Федерации по сохранению и укреплению традиционных российских духовно-нравственных ценностей (далее – государственная политика по сохранению и укреплению традиционных ценностей) представляет со-

бой совокупность скоординированных мер, осуществляемых Президентом Российской Федерации и иными органами публичной власти при участии институтов гражданского общества для противодействия социокультурным угрозам национальной безопасности Российской Федерации в части, касающейся защиты традиционных ценностей.

10. Государственная политика по сохранению и укреплению традиционных ценностей реализуется в области образования и воспитания, работы с молодежью, культуры, науки, межнациональных и межрелигиозных отношений, средств массовой информации и массовых коммуникаций, международного сотрудничества. В реализации такой государственной политики участвуют федеральные органы исполнительной власти, ведающие вопросами обороны, безопасности государства, внутренних дел, общественной безопасности, и иные органы публичной власти в пределах своих полномочий.

II. Оценка ситуации, основные угрозы и риски для традиционных ценностей, сценарии развития ситуации

11. Усилия, предпринимаемые Российской Федерацией для развития духовного потенциала ее народа, способствуют повышению сплоченности российского общества, осознанию гражданами необходимости сохранения и укрепления традиционных ценностей в условиях глобального цивилизационного и ценностного кризиса, ведущего к утрате человечеством традиционных духовно-нравственных ориентиров и моральных принципов.

12. В Стратегии национальной безопасности Российской Федерации ситуация в России и в мире оценивается как требующая принятия неотложных мер по защите традиционных ценностей.

13. Угрозу традиционным ценностям представляют деятельность экстремистских и террористических организаций, отдельных средств массовой информации и массовых коммуникаций, действия Соединенных Штатов Америки и других недружественных иностранных государств, ряда транснациональных корпораций и иностранных некоммерческих организаций, а также деятельность некоторых организаций и лиц на территории России.

14. Идеологическое и психологическое воздействие на граждан ведет к насаждению чуждой российскому народу и разрушительной

для российского общества системы идей и ценностей (далее – деструктивная идеология), включая культивирование эгоизма, вседозволенности, безнравственности, отрицание идеалов патриотизма, служения Отечеству, естественного продолжения жизни, ценности крепкой семьи, брака, многодетности, созидательного труда, позитивного вклада России в мировую историю и культуру, разрушение традиционной семьи с помощью пропаганды нетрадиционных сексуальных отношений.

15. Деструктивное идеологическое воздействие на граждан России становится угрозой для демографической ситуации в стране.

16. Деятельность публично-правовых образований, организаций и лиц, способствующая распространению деструктивной идеологии, представляет объективную угрозу национальным интересам Российской Федерации.

17. Распространение деструктивной идеологии влечет за собой следующие риски:

а) создание условий для саморазрушения общества, ослабление семейных, дружеских и иных социальных связей;

б) усиление социокультурного расслоения общества, снижение роли социального партнерства, обесценивание идей созидательного труда и взаимопомощи;

в) причинение вреда нравственному здоровью людей, навязывание представлений, предполагающих отрицание человеческого достоинства и ценности человеческой жизни;

г) внедрение антиобщественных стереотипов поведения, распространение аморального образа жизни, вседозволенности и насилия, рост употребления алкоголя и наркотиков;

д) формирование общества, пренебрегающего духовно-нравственными ценностями;

е) искажение исторической правды, разрушение исторической памяти;

ж) отрицание российской самобытности, ослабление общероссийской гражданской идентичности и единства многонационального народа России, создание условий для межнациональных и межрелигиозных конфликтов;

з) подрыв доверия к институтам государства, дискредитация идеи служения Отечеству, формирование негативного отношения к воинской службе и государственной службе в целом.

18. В целях сохранения и укрепления традиционных ценностей, пресечения распространения деструктивной идеологии реформы в области образования и воспитания, культуры, науки, средств массовой информации и массовых коммуникаций должны проводиться с учетом исторических традиций и накопленного российским обществом опыта при условии проведения широкого общественного обсуждения.

19. Решение проблем в области сохранения и укрепления традиционных ценностей должно осуществляться по следующим основным направлениям:

а) корректировка документов стратегического планирования в целях более эффективного решения задач по сохранению и укреплению традиционных ценностей, определения ориентиров для выбора целей и наиболее эффективных механизмов обеспечения национальных интересов в данной области;

б) обеспечение межведомственной координации деятельности по защите традиционных ценностей;

в) совершенствование системы государственной поддержки проектов в области культуры и образования с учетом целей государственной политики по сохранению и укреплению традиционных ценностей;

г) развитие и совершенствование форм и методов противодействия рискам, связанным с распространением деструктивной идеологии в информационном пространстве;

д) совершенствование форм и методов воспитания и образования детей и молодежи в соответствии с целями государственной политики по сохранению и укреплению традиционных ценностей;

е) повышение эффективности деятельности научных, образовательных, просветительских организаций и организаций культуры по защите исторической правды, сохранению исторической памяти, противодействию фальсификации истории;

ж) совершенствование деятельности правоохранительных органов по профилактике и пресечению противоправных действий, направленных на распространение деструктивной идеологии.

20. В дальнейшем ситуация может развиваться по позитивному либо негативному сценарию.

21. Позитивный сценарий будет реализован при условии системного и последовательного проведения государственной политики по сохранению и укреплению традиционных ценностей. Данный сценарий предполагает усиление защищенности российского общества от угроз и рисков для традиционных ценностей. Он ориентирован на формирование высоконравственной личности, воспитанной в духе уважения к традиционным ценностям, обладающей актуальными знаниями и умениями, способной реализовать свой потенциал в условиях современного общества, готовой к мирному созиданию и защите Отечества. Позитивный сценарий предполагает постепенное преодоление существующих проблем, поиск ответов на новые вызовы исходя из традиционных ценностных ориентиров.

22. Негативный сценарий может быть реализован в случае отсутствия противодействия распространению деструктивной идеологии.

III. Цели и задачи государственной политики по сохранению и укреплению традиционных ценностей

23. Целями государственной политики по сохранению и укреплению традиционных ценностей являются:

а) сохранение и укрепление традиционных ценностей, обеспечение их передачи от поколения к поколению;

б) противодействие распространению деструктивной идеологии;

в) формирование на международной арене образа Российского государства как хранителя и защитника традиционных общечеловеческих духовно-нравственных ценностей.

24. Реализация стратегического национального приоритета «Защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти» предполагает решение следующих задач государственной политики по сохранению и укреплению традиционных ценностей:

а) укрепление гражданского единства, общероссийской гражданской идентичности и российской самобытности, межнационально-

го и межрелигиозного согласия на основе объединяющей роли традиционных ценностей;

б) сохранение исторической памяти, противодействие попыткам фальсификации истории, сбережение исторического опыта формирования традиционных ценностей и их влияния на российскую историю, в том числе на жизнь и творчество выдающихся деятелей России;

в) сохранение, укрепление и продвижение традиционных семейных ценностей (в том числе защита института брака как союза мужчины и женщины), обеспечение преемственности поколений, забота о достойной жизни старшего поколения, формирование представления о сбережении народа России как об основном стратегическом национальном приоритете;

г) реализация государственной информационной политики, направленной на усиление роли традиционных ценностей в массовом сознании и противодействие распространению деструктивной идеологии;

д) воспитание в духе уважения к традиционным ценностям как ключевой инструмент государственной политики в области образования и культуры, необходимый для формирования гармонично развитой личности;

е) поддержка общественных проектов и институтов гражданского общества в области патриотического воспитания и сохранения историко-культурного наследия народов России;

ж) поддержка религиозных организаций традиционных конфессий, обеспечение их участия в деятельности, направленной на сохранение традиционных ценностей, противодействие деструктивным религиозным течениям;

з) формирование государственного заказа на проведение научных исследований, создание информационных и методических материалов (в том числе кинолетописи и других аудиовизуальных материалов), произведений литературы и искусства, оказание услуг, направленных на сохранение и популяризацию традиционных ценностей, а также обеспечение контроля качества выполнения этого государственного заказа;

и) обеспечение государственной охраны объектов культурного наследия (памятников истории и культуры) народов Российской Федерации, предоставление доступа к ним в целях их популяризации как

среды, формирующей историческое самосознание, воспитывающей любовь и уважение к Отечеству;

к) поддержка проектов, направленных на продвижение традиционных ценностей в информационной среде;

л) защита и поддержка русского языка как языка государствообразующего народа, обеспечение соблюдения норм современного русского литературного языка (в том числе недопущение использования нецензурной лексики), противодействие излишнему использованию иностранной лексики;

м) защита от внешнего деструктивного информационно-психологического воздействия, пресечение деятельности, направленной на разрушение традиционных ценностей в России;

н) повышение роли России в мире за счет продвижения традиционных российских духовно-нравственных ценностей, основанных на исконных общечеловеческих ценностях.

IV. Инструменты реализации государственной политики по сохранению и укреплению традиционных ценностей

25. Правовыми инструментами реализации государственной политики по сохранению и укреплению традиционных ценностей являются:

а) совершенствование нормативно-правовой базы на федеральном, региональном и муниципальном уровнях;

б) разработка органами публичной власти документов стратегического планирования с учетом целей и задач государственной политики по сохранению и укреплению традиционных ценностей.

26. Основными организационными инструментами реализации государственной политики по сохранению и укреплению традиционных ценностей являются:

а) разработка органами публичной власти планов мероприятий по реализации настоящих Основ;

б) оценка проектов (в том числе информационных и иных материалов), программ и мероприятий на предмет соответствия традиционным ценностям при решении вопроса о целесообразности их государственной поддержки;

в) мониторинг достижения целей государственной политики по сохранению и укреплению традиционных ценностей, в том числе выполнения планов мероприятий по реализации настоящих Основ;

г) осуществление органами публичной власти контроля за соответствием финансируемых за счет средств бюджетов бюджетной системы Российской Федерации мероприятий целям и задачам государственной политики по сохранению и укреплению традиционных ценностей;

д) привлечение институтов гражданского общества, в том числе религиозных организаций, к участию в реализации государственной политики по сохранению и укреплению традиционных ценностей.

27. Научно-аналитическими инструментами реализации государственной политики по сохранению и укреплению традиционных ценностей являются:

а) проведение исследований по вопросам, связанным с реализацией государственной политики по сохранению и укреплению традиционных ценностей на федеральном, региональном и муниципальном уровнях, включая оценку эффективности реализации соответствующих программ и проектов;

б) разработка методических рекомендаций по реализации государственной политики по сохранению и укреплению традиционных ценностей.

28. Информационным инструментом реализации государственной политики по сохранению и укреплению традиционных ценностей является взаимодействие органов публичной власти со средствами массовой информации и массовых коммуникаций в целях популяризации и продвижения традиционных ценностей.

29. Мониторинг достижения целей государственной политики по сохранению и укреплению традиционных ценностей требует разработки соответствующей системы показателей, основанных на следующих данных:

а) официальная статистическая информация;

б) итоги социологических исследований;

в) результаты мониторинга проблемных ситуаций, связанных с сохранением и укреплением традиционных ценностей (по субъектам Российской Федерации и сферам ответственности органов публичной власти).

30. Финансовое обеспечение мероприятий по реализации государственной политики по сохранению и укреплению традиционных ценностей осуществляется за счет средств бюджетов бюджетной системы Российской Федерации, а также за счет иных источников финансирования в случаях, предусмотренных законодательством Российской Федерации. При этом подготовка проектов бюджетов бюджетной системы Российской Федерации должна осуществляться с учетом целей и задач этой государственной политики.

V. Ожидаемые результаты реализации государственной политики по сохранению и укреплению традиционных ценностей

31. Реализация государственной политики по сохранению и укреплению традиционных ценностей будет способствовать сбережению и приумножению народа России, сохранению общероссийской гражданской идентичности, развитию человеческого потенциала, поддержанию гражданского мира и согласия в стране, укреплению законности и правопорядка, формированию безопасного информационного пространства, защите российского общества от распространения деструктивной идеологии, достижению национальных целей развития, повышению конкурентоспособности и международного престижа Российской Федерации.

32. По результатам оценки эффективности реализации государственной политики по сохранению и укреплению традиционных ценностей положения настоящих Основ при необходимости подлежат корректировке не реже одного раза в шесть лет.

Учебное электронное издание

ЮДИНА Анна Михайловна

ОСНОВЫ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ
ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ (КИБЕРСРЕДА)
В ОБРАЗОВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Учебное пособие

Редактор Е. А. Лебедева

Технические редакторы Ш. Ш. Амирсейидов, Н. В. Пустовойтова

Компьютерная верстка Л. В. Макаровой

Корректор О. В. Балашова

Выпускающий редактор А. А. Амирсейидова

Системные требования: Intel от 1,3 ГГц; Windows XP/7/8/10; Adobe Reader; дисковод CD-ROM.

Тираж 9 экз.

Издательство Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых.
600000, Владимир, ул. Горького, 87.