13/23
ПРЕПРИНТЫ

ЦИФРОВОЕ ОБЩЕСТВО И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ИННОВАЦИИ
DIGITAL SOCIETY AND INFORMATION TECHNOLOGIES INNOVATIONS

ЦИФРОВОЕ ОБЩЕСТВО И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ. ИННОВАЦИИ
DIGITAL SOCIETY AND INFORMATION TECHNOLOGIES INNOVATIONS

О. В. Шмалий, О. В. Гречкина, Л. А. Душакова
И. В. Котов, А. В. Хромова

СОВЕРШЕНСТВОВАНИЕ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИЩЕННОСТИ ЛИЧНОСТИ ОТ ИНФОРМАЦИОННЫХ УГРОЗ В ЦИФРОВОЙ СРЕДЕ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (РАНХиГС)

Шмалий О.В., Гречкина О.В., Душакова Л.А., Котов И.В., Хромова А.В.

СОВЕРШЕНСТВОВАНИЕ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ЗАЩИЩЕННОСТИ ЛИЧНОСТИ ОТ ИНФОРМАЦИОННЫХ УГРОЗ В ЦИФРОВОЙ СРЕДЕ

Руководитель НИР, заведующий кафедрой административного и информационного права ИПНБ РАНХиГС, д.ю.н., профессор	Шмалий О.В. (ORCID – 0000-0002-3492-5381; shmaliy-ov@ranepa.ru)
Исполнители: профессор кафедры административного и информационного права ИПНБ РАНХиГС, д.ю.н., профессор	Гречкина О.В. (ORCID-0000-0002-3802-2323; grechkina-ov@ranepa.ru)
заведующий кафедрой административного и служебного права ЮРИУ РАНХиГС, д.ю.н., доцент	Душакова Л.А. (ORCID - 0000-0002-2613-4280 dushakova-la@ranepa.ru)
аспирант РАНХиГС	Котов И.В. ikotov-17-01@edu.ranepa.ru
аспирант РАНХиГС	Хромова А.В. (ORCID-0000-0003-3329-3682; atarasenko-16-01@edu.ranepa.ru)

Москва 2023

Аннотация

Актуальность. В условиях нарастающего негативного трансграничного оборота информации в террористических, экстремистских и иных противоправных целях, особую актуальность приобретает исследование правовых механизмов защищенности личности от информационных угроз в цифровой среде, которые позволят противостоять информационно-психологическому воздействию, пропаганде экстремистской идеологии, распространению ксенофобии, идей национальной исключительности.

Цель работы – сформировать предложения по совершенствованию правового регулирования защищенности личности от информационных угроз в цифровой среде с учетом современных вызовов и угроз**.**

Объект исследования – общественные отношения в области информационной безопасности, возникающие в связи с обеспечением защищенности личности от информационных угроз в цифровой среде.

Методы исследования. Общенаучные методы: системный анализ и синтез, диалектическое познание, логический, статистический, сравнительный, моделирования. Частно-научные методы: формально-юридический, сравнительно-правовой, системно-догматическое толкование.

Научная новизна заключается в комплексном исследовании правовых механизмов обеспечения состояния защищенности личности от информационных угроз в цифровой среде, ориентированным на обоснование и разработку предложений по совершенствованию правового регулирования защищенности личности от информационных угроз в цифровой среде.

Результаты работы могут быть использованы в интересах государственных органов и органов исполнительной власти, наделенных полномочиями в области обеспечения защищенности личности от информационных угроз в цифровой среде, а также в интересах Академии для развития научного потенциала в целях повышения качества экспертно-аналитической работы и образовательных программ.

Ключевые слова: законодательство, цифровая среда, информационные угрозы, информационно-мировоззренческая безопасность, защищенность личности, антикоррупционный механизм, общество, ответственность.

Federal State Budgetary Educational Institution
of Higher Education
"Russian Academy of National Economy and Public Administration
under the President of the Russian Federation" (RANEPA)

Shmaliy O.V., Grechkina O.V., Dushakova L.A., Kotov I.V., Khromova A.V.

IMPROVEMENT OF LEGISLATION IN THE FIELD OF PERSONAL PROTECTION FROM INFORMATION THREATS IN THE DIGITAL ENVIRONMENT

Head of research, Head of the Department of Administrative and Information Law, IPNB RANEPA, Doctor of Law, Professor	Shmaliy O.V. (ORCID – 0000-0002-3492-5381; shmaliy-ov@ranepa.ru)
Performers: Professor of the Department of Administrative and Information Law, IPNB RANEPA, Doctor of Law, Professor	Grechkina O.V. (ORCID - 0000-0002-3802-2323; grechkina-ov@ranepa.ru)
Head of the Department of Administrative and Service Law of the YuRIU RANEPA, Doctor of Law, Associate Professor	Dushakova L.A. (ORCID - 0000-0002-2613-4280 dushakova-la@ranepa.ru)
postgraduate student at RANEPA	Kotov I.V. ikotov-17- 01@edu.ranepa.ru
postgraduate student at RANEPA	Khromova A.V. (ORCID- 0000-0003-3329-3682; atarasenko-16- 01@edu.ranepa.ru)

Moscow 2023

Annotation

Relevance. In the context of the growing negative cross-border circulation of information for terrorist, extremist and other illegal purposes, the study of legal mechanisms of personal protection from information threats in the digital environment, which will allow to resist information and psychological influence, propaganda of extremist ideology, the spread of xenophobia, ideas of national exclusivity, is of particular relevance.

The purpose of the work is to form proposals for improving the legal regulation of personal protection from information threats in the digital environment, taking into account modern challenges and threats.

The object of the study is public relations in the field of information security arising in connection with ensuring the protection of the individual from information threats in the digital environment.

Research methods. General scientific methods: system analysis and synthesis, dialectical cognition, logical, statistical, comparative, modeling. Private-scientific methods: formal-legal, comparative-legal, systemic-dogmatic interpretation.

The scientific novelty consists in a comprehensive study of the legal mechanisms for ensuring the state of personal protection from information threats in the digital environment, focused on the justification and development of proposals for improving the legal regulation of personal protection from information threats in the digital environment.

The results of the work can be used in the interests of state bodies and executive authorities authorized to ensure the protection of the individual from information threats in the digital environment, as well as in the interests of the Academy for the development of scientific potential in order to improve the quality of expert and analytical work and educational programs.

Keywords: legislation, digital environment, information threats, information and ideological security, personal security, anti-corruption mechanism, society, responsibility.

ВВЕДЕНИЕ

Информационная безопасность стала неотъемлемой составляющей человеческой жизнедеятельности. Решение проблем обеспечения информационной безопасности базируется на понимании сущности глобального информационного пространства, которое продолжает формироваться в ходе информационной революции и неуклонно становится сферой непрерывно увеличивающегося многообразия информационных угроз. Социальные связи в онлайн социальных сообществах сформировали особый виртуальный мир, который имеет собственный этикет, систему ценностей, язык и формы поведения, в том числе, девиантного, и при этом является экстерриториальным и, по большей части, анонимным, что, в свою очередь, и запускает механизмы асоциального поведения, включая пропаганду радикальных и общественно опасных идей.

Появление специфической сетевой культуры обуславливает новые социальные риски, которые должны быть приняты во внимание при формировании правового регулирования в этой сфере социального бытия, которая достаточно сложно поддается законодательному и правоприменительному опосредованию; многие вопросы в этой сфере требуют юридического осмысления и закрепления. Особенно это касается гармонизации права на свободу слова и плюрализм мнений и права на безопасную коммуникацию, защиту общественной безопасности и общественного порядка, территориальной целостности государства и т. д. в связи с распространением деструктивной и криминогенной информации, которая обладает высокой степенью общественной опасности.

В рамках представленного исследования предпринята попытка обобщения действующего законодательства и правоприменительной практики в области информационной безопасности, разработаны предложения по модернизации действующего законодательства и повышению эффективности и результативности мер, направленных по совершенствование правового регулирования защищенности личности от информационных угроз в цифровой среде с учетом современных вызовов и угроз, а также тенденций развития национальной правовой системы и публичного управления.

1 Теоретико-методологические и организационно-правовые основы защищенности личности от информационных угроз в цифровой среде

1.1 Информационная безопасность в контексте идеалов и принципов прав человека

В рамках российской национальной правовой системы действует значительное число актов нормативного регулирования в области персональных данных, включая законы (прежде всего, профильный федеральный закон о персональных данных) и подзаконные акты, включая акты профильных исполнительно-распорядительных органов. В то же время сложных моментов и «узких мест» в действующем законодательстве достаточно много. В частности, спорным является вопрос об объеме и содержании информации, которую можно отнести к персональным данным, что не редко приводит к тактической интерпретации соответствующей информации в правоприменительной практике в случае возникновения конкретного спора. Соответственно, человек сталкивается с ситуацией, когда он прежде всего сам должен обеспечить безопасность своих данных и нести ответственность за их предоставление, понимая, что участие в отношениях, основанных на использовании цифровых технологий, неизбежно приводит к заведомой необходимости добровольного предоставления данных, не имея последующей возможности отслеживать их судьбу. И здесь возникает позиция выбора для субъекта персональных данных: предоставить данные или отказаться от участия в том или ином отношении. Также сложность вызывает массовость обработки персональных данных, что усложняет достижение надлежащего уровня эффективности и результативности контроля в этой сфере со стороны государства.

Нельзя забывать и о многочисленных фактах утечки персональных данных, в том числе со стороны тех лиц, которые обязаны обеспечивать их защиту, что снижает уровень доверия граждан к государству как субъекту, которой имеет все прерогативы по регулированию оборота персональных данных и их защите. И это приобретает еще большую актуальность в связи с формированием Единой биометрической системы. Кроме того, утечка данных составляет весьма значимый бизнес-ресурс. Представляется, что единственно возможным на данном этапе решением вопроса минимизации утечек является совершенствование мер идентификации и аутентификации, поскольку способы кражи персональных данных развиваются и достичь их абсолютной защищенности, по крайней мере на текущем технологическом этапе, просто

невозможно, соответственно, приоритетными должны стать меры профилактики и цифровой гигиены. Особое значение в контексте защиты идеалов и принципов прав человека приобретают различные формы воздействия на когнитивный и психологический строй личности в целях трансформации его мировоззрения в целом.

Безусловно, все изложенное требует ответа со стороны государства и специальной нормативной регуляции. Отсутствие программно-ценностной и стратегической цельности в этом направлении также является одной из причин недостаточности текущего правового регулирования. Комплексно регулирование может быть сформировано только при ясной общей, официально признанной идеологии и философии прав человека и их защиты в цифровой среде.

Еще одним сложным вопросом, который непосредственно связан с идеалами и принципами прав человека в контексте информационной безопасности, выступает конфликт аксиологии конституционных основ устройства государства и общества и идеологии цифровизации как таковой: ускоренная тотальная цифровизация неизбежно создает легитимацию информационно-цифровой небезопасности, а, следовательно, сама по себе является мировоззренческой угрозой. Недостаточность концептуализации цифровизации как явления и создаваемых ею угроз влечет повышенные риски жизнедеятельности личности, общества и государства во многих смыслах, прежде всего, в части неуклонного повышения коррупциогенности цифровой среды, включая повышение коррупционных рисков. Негативные эффекты вызывает и отсутствие ответственности, причем не в плане отсутствия соответствующей нормативной основы, а в плане правоприменения, то есть фактического отсутствия наказуемости. Кроме того, специалисты отмечают низкий уровень надежности хранения документов в цифровой форме (срок жизни цифровых форматов и носителей информации, операционных систем, уязвимость ИТ-инфраструктуры, как технологическая, так и физическая) и необходимость постоянного резервирования. В этой связи как минимум рано признавать единственным оригиналом цифровой документ, соответственно, документооборот должен иметь гибридный электронно-бумажный характер.

Вопросы информационной безопасности в контексте идеалов и принципов прав человека также непосредственно связаны с идеей цифрового суверенитета как необходимой составляющей национального суверенитета. Проблематика цифрового суверенитета обостряется подходом к правам человека как универсальному концепту, имеющему наднациональный характер в силу всеобщности их декларирования и признания и способному, в этой связи, ограничивать государственный суверенитет. При этом ряд универсальных прав

человека, которые имеют также национальное конституционное провозглашение, теперь имеют новое содержательное наполнение, вытекающее из новой цифровой реальности.

Все сказанное позволяет говорить о необходимости конструирования национальной модели цифровизации и цифровой безопасности, способную обеспечить права граждан и национальный суверенитет, имеющую общественную поддержку и необходимое программно-ценностное, нормативно-правовое и институциональное сопровождение.

Направления совершенствования организационно-правовой основы информационной безопасности в контексте идеалов и принципов прав человека могут быть представлены следующим образом:

– разработка новой концептуально-ценностной основы (стратегии) обеспечения информационной безопасности, учитывая сформулированные выше постулаты;

– разработка правового механизма противодействия негативному информационному воздействию и информационному насилию, в том числе, путем усиления ответственности за правонарушения в цифровой среде и с использованием цифровых технологий;

– разработка правового механизма независимой экспертизы и независимого аудита в области цифровых технологий, защиты приватности, негативного информационного воздействия и информационного насилия; общественно значимые проекты и программы цифровизации проводить через такого рода экспертизу;

– запрет цифровой дискриминации;

– совершенствование мер идентификации и аутентификации в целях решения вопроса минимизации утечек персональных данных;

– запрет ограничения личного цифрового суверенитета.

1.2 Законодательство в области защищенности личности от информационных угроз в цифровой среде

Отношения в области обеспечения информационной безопасности регулируются в соответствии с Конституцией Российской Федерации, общепризнанными принципами и нормами международного права, Федеральными законами, другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами.

Закон 187-ФЗ определяет основные принципы обеспечения безопасности, предназначение государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на

территории Российской Федерации, категорирует объекты критической информационной инфраструктуры, устанавливает обязанность федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации вести реестр значимых объектов критической информационной инфраструктуры, полномочия Президента Российской Федерации и органов государственной власти, права, обязанности субъектов и ответственность за нарушение требований законодательства, устанавливает критерии значимости и показатели их значений, в целях учета значимых объектов – обязанность ведения реестра значимых объектов, а также обязанность осуществления федеральным органом исполнительной власти оценки безопасности и государственного контроля безопасности.

Принятие закона 187-ФЗ неизбежно повлекло изменения в соответствующие кодифицированные законы. Так Уголовный кодекс Российской Федерации дополнен статьей 274.1, которая за «создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты информации» предусматривает наказание в виде принудительных работ с ограничением свободы либо лишение свободы с установленным размером штрафа.

Также, на наш взгляд особенно необходимым в существующих реалиях правоприменительной практики государственных органов и их должностных лиц в сфере защищенности личности от информационных угроз является увеличение количества составов административных правонарушений. Предусмотренные главой 13 КоАП РФ «Административные правонарушения в области связи и информации» правонарушения (в области связи; в области средств массовой информации; в области порядка сбора, хранения, использования, распространения и защиты информации) к субъектам административной ответственности относят: операторов связи; организаторов распространения информации в информационно-телекоммуникационной сети Интернет; владельцев новостного агрегатора; организаторов сервиса обмена мгновенными сообщениями; операторов поисковой системы; владельцев сайтов и других.

Раскрывая содержание законодательства в области защищенности личности от информационных угроз в цифровой среде, необходимо говорить о том, что главной его задачей считается нормативная регламентация государственного управления через издание актов управления. К таким актам можно отнести подзаконные правовые акты органов

государственной власти. Правовую основу Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации составляют Конституция Российской Федерации, федеральные законы, Стратегия национальной безопасности Российской Федерации до 2020 года, Доктрина информационной безопасности Российской Федерации. Концепцией также определены назначение, функции и принципы создания государственной Системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Важную роль в области защищенности личности от информационных угроз в цифровой среде играют нормативные акты Правительства Российской Федерации, которыми утверждены правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, правила подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры, правила формирования и утверждения перечня критически важных объектов, правила категорирования объектов критической информационной инфраструктуры и перечня показателей критериев значимости таких объектов, и что не менее важно – перечень ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищённости своих информационных систем с привлечением организаций, имеющих соответствующие лицензии.

Для обеспечения нормативных требований для создания и функционирования системы защиты критической информационной инфраструктуры приняты ведомственные акты, которыми утвержден порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры, требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования.

В контексте исследования защищенности личности от информационных угроз отметим, что государственное регулирование отношений в сфере защищенности личности от информационных угроз выражается в установлении требований по защите информации, во введении ответственности за нарушение законодательства Российской Федерации, которые в

полной мере соответствуют требованиям правового государства и современным вызовам демократического развития.

В этой связи, представляется, законодателю необходимо отказаться от использования оценочных категорий, что, в свою очередь, может позитивно повлиять на преодоление сложностей в их квалификации. Соответствующее разъяснение Пленума Верховного Суда Российской Федерации, может быть посвящено информационным правонарушениям, положения которого могли бы поспособствовать единообразному применению норм административного законодательства.

1.3 Спецификация информационных угроз личности в цифровой среде

Спецификация информационных угроз личности в цифровой среде в целом уже достаточно проработана в различных источниках. В то же время эта спецификация не может рассматриваться как стабильная, поскольку динамика развития цифровой среды непрерывно увеличивается, и тенденции такого развития позволяют предполагать появление все новых угроз личности, обществу и государству.

В целом, область киберугроз сложно поддается надлежащему противодействию со стороны правоохранительных органов. Несмотря на то, что в целом есть возможность вычислить анонимного правонарушителя, их количество является чрезмерно большим по сравнению с возможностями правоохранительных органов.

Еще одной проблемой, актуальность которой неуклонно возрастает, являются так называемые thrash stream. Действующее российское законодательство располагает достаточным объемом регулирования по противодействию распространению посредством информационно-телекоммуникационных сетей негативных информационных материалов, в том числе трансляций в режиме реального времени или публикаций видеозаписей, направленных на унижение человеческого достоинства и публичную демонстрацию насильственных действий.

Таким образом, можно полагать, что противодействие так называемым thrash stream в целом обеспечено необходимыми правовыми механизмами. Также следует отметить, что формирование специального регулирования, в том числе разработка терминологии в той сфере отношений, которая, с одной стороны, непрерывно развивается, а во-вторых, имеет достаточную правовую определенность, вряд ли целесообразно, особенно в связи с особой динамикой появления новых явлений в цифровом пространстве (есть существенный риск

разработать понятие, которое весьма скоро может утратить свою актуальность, как минимум, в силу изменения формата содержания и распространения).

Проблему безопасности в цифровой среде составляет технология deepfake. Нормативно-регулятивное опосредование создания и распространения «дипфейков» фактически является слабым и недостаточным. В то же время очевидно, что эта технология способна существенным образом повлиять не только на юридические, но и на морально-психологическое состояние человека. Одним из решений здесь также является автоматическая оценка регулятором и площадкой признаков указанных манипуляций. Но этот вопрос должен быть разрешен не только технически, но и юридически, что предполагает необходимость разработки правового механизма противодействия распространению deepfake.

В связи с вышеизложенным следует обратить внимание на то, что в правовой доктрине уже формируется специфическая терминология - информационный вандализм (объединяет деструктивные действия в отношении информации и информационной среды), информационный криминал, информационный терроризм, которые, среди прочего, обладают высокой степенью информационно-психологической и когнитивной опасности. И в этой связи должен быть решен вопрос методологии и методик выявления такого рода риской и угроз, поскольку традиционные методики, основанные на цензуре, не являются достаточными, прежде всего, в силу их субъективности, а равно длительности практической реализации. В данном случае речь должна идти о методиках оперативного вскрытия деструктивной информации широкого круга влияния, причем, в том числе, в условиях отсутствия ее непосредственного влияния (потенциальное влияние), что позволит существенно увеличить возможности снятия конфликтности в социуме.

Обобщая вышесказанное, представляется возможным сделать ряд выводов.

1. Терминология, используемая при обозначении цифровых угроз личности, неуклонно расширяется, при этом в правовую сферу она проникает не активно, по большей части в порядке рекомендательного регулирования.

2. Деяние в форме кибербуллинга в целом подпадает под административную ответственность за оскорбление в соответствии со статьей 5.61 КоАП РФ, но при этом понятие кибербуллинга имеет акценты квалификации, которые позволяют рассматривать его как квалифицированное оскорбление с возможностью применения более серьезных мер реагирования.

3. На сегодняшний день киберугрозы создают значительные проблемы противодействия таким угрозам со стороны правоохранительных органов. В этой связи представляется

целесообразным сформулировать новый образовательный стандарт и соответствующие образовательные программы подготовки правоохранителей с IT-специализацией.

Кроме того, в силу повышающейся актуальности речеведческих экспертиз, результатом которых является установление диагностически значимых признаков собственно вербального поведения, образующего состав правонарушения, а равно в силу полиспециализации таких экспертиз, представляется целесообразным сформулировать самостоятельную образовательную программу высшего образования.

4. Правовой режим противодействия thrash stream имеет существенные ресурсы для последовательного совершенствования используемых правовых механизмов, что позволяет ставить вопрос комплексно о реакции государства не столько в рамках формирования специальной конструкции ответственности, что, безусловно, должно быть, сколько о формировании комплексной государственной программы профилактики распространения виртуальной thrash-реальности и преодоления соответствующих последствий, включая механизмы психологической реабилитации.

5. Помимо решения задач концептуального, стратегического и текущего нормативно-регулятивного характера, следует говорить о необходимости разработки комплексной теоретико-методологической модели видов информационных угроз (понятие угрозы, цели, задачи и условия ее проявления, механизм причинно-следственных связей, методы, силы и средства противодействия, показатели и критерии его эффективности; критерии и свойства объектов защиты).

1.4 Теоретико-методологическое обоснование понятия «информационно-мировоззренческая безопасность»

Понятие информационно-мировоззренческой безопасности включает две взаимосвязанные составляющие – информационную и мировоззренческую. И если первая имеет в целом достаточно сформированное и очевидное юридическое содержание, то вторая крайне затруднительна для юридического опосредования.

Важным является соотношение понятий мировоззрения и идеологии, которые, при всей содержательной близости, нельзя признать совпадающими. В частности, элементы мировоззрения и идеологии могут совпадать, если говорить о религиозном мироощущении, мировосприятии и миропонимании, а равно могут состоять в антагонизме, если говорить о возможных противоречиях политической идеологии и научного мировоззрения (чему есть исторические примеры идеологизации научного знания и научного развития, в том числе из

советской истории). Идеология в значительно большей мере субъективна по сравнению с мировоззрением. Принципиальным отличием идеологии от мировоззрения является определенная искусственность первой.

Следует отметить, что в нормативном поле термин (слово) «идеология» используется достаточно активно, но абсолютно контекстуально. Национальная правовая система включает достаточное количество правовых актов различных юридических свойств в области противодействия идеологии терроризма и экстремизма, коррупции, ксенофобии, национализма, политического террора, включая акты международно-правового регулирования и федеральные законы, в том числе законы об ответственности (УК РФ и КоАП РФ). Кроме того, можно указать на конкретные нормативные дефиниции идеологии определенного содержания, как правило. в актах стратегического планирования и программно-ценностных актах: антинаркотическая идеология [93], идеология насилия [94] - в обоих случаях речь идет о совокупности взглядов и идей, но с различной основой (позитивной / негативной).

Наиболее активно мировоззренческие парадигмы проявляются в сфере обеспечения информационной безопасности как идея воспитания и продвижения толерантности социальных активностей и взаимосвязей, которая имеет прямую связь с образованием в единстве обучения и воспитания, поскольку именно образование призвано транслировать то, что сейчас принято называть «мировоззренческим кодом», через систему специализированных институтов передачи любого социально значимого опыта (национального, государственного, общечеловеческого) в тех или иных формах в целях обеспечения преемственности поколений. Соответственно, современные образовательные стратегии, технологии и институты должны выстраиваться в таком контексте, который позволит обеспечить в наибольшей мере достоверную трансляцию «мировоззренческого кода», а это, в свою очередь, предполагает определенную унификацию образовательных программ всех образовательных уровней и формирование ядра (основы) единства образовательного пространства в целях формирования и стабилизации гражданской идентичности на основе определенной ценностной системы.

«Мировоззренческий код» формируется, прежде всего, в рамках, которые дополняются идеей равенства образования вне зависимости от каких-либо биологических, социально-культурных, политических, ценностных и иных особенностей и которые задают систему знаний, убеждений, идеалов и ценностей как основу взаимодействия «гражданин – государство», «гражданин в государстве», используя единообразные и опознаваемые социально-культурные и ценностные понятийные ряды, что, в свою очередь, создает устойчивость общественно-политического устройства и является фактором политико-правового и социально-экономического развития и национальной безопасности.

Следует отметить, что в нормативном поле термин (слово) «мировоззрение», также, как и термин (слово) «идеология», используется достаточно активно, но абсолютно контекстуально и в отсутствии попыток дефиниции. Формирование мировоззрения транслируется как одна из задач образования в сфере культуры и искусства [129], как одной из приоритетных направлений фундаментальных и поисковых научных исследований на 2021 - 2030 годы [130].

Таким образом, можно наблюдать отсутствие понятия мировоззрения и его концептуального осмысления в рамках национальной правовой системы. При этом очевидно, что мировоззрение есть результат информационного воздействия на индивида, социальные группы и общество в целом, соответственно, вопросы информационной политики напрямую взаимосвязаны с вопросами политики мировоззренческой, что позволяет говорить не просто об информационной безопасности, а об информационно-мировоззренческой безопасности.

Кроме того, решение вопросов информационно-мировоззренческой безопасности предполагает формулирование и конкретизацию соответствующих угроз, которые могут быть внутренними и внешними, намеренными (организованными) и непреднамеренными (стихийными), явными и латентными и так далее. Эта позиция является принципиально важной, поскольку те угрозы, с которыми в настоящее время сталкивается Российская Федерация, имеют принципиально новый уровень, требующий их адекватной оценки, ответа и нейтрализации.

В этой связи представляется целесообразным сделать следующие выводы и предложения.

1. Признание информационно-мировоззренческой безопасности в качестве самостоятельного правового института должно состояться, прежде всего, в рамках стратегического планирования.

2. На сегодняшний день, исходя из положений о федеральных органах исполнительной власти, нет уполномоченного органа, компетенцию которого оставляют вопросы мировоззренческой безопасности, информационного противоборства и гибридных войн. По всей видимости, создавать специализированный орган исполнительной власти нецелесообразно, но сформулировать область функций и конкретные полномочия возможно в отношении уже действующих уполномоченных в области обеспечения безопасности и обороны, цифрового развития и информационных технологий органов.

3. Признание информационно-мировоззренческой безопасности в качестве самостоятельного правового института предполагает не только планово-стратегическое, но и конкретное нормативное сопровождение. В этой связи систематизация необходимых нормативных положений возможна только в порядке принятия специального федерального

закона, что будет являться следствием принятия Доктрины мировоззренческой безопасности. Также принятие такого закона потребует новых редакций тех законодательных актов, которые непосредственно коррелируют с вопросами информационной безопасности.

4. В образовательные стандарты и образовательные программы среднего профессионального и высшего образования в области государственного и муниципального управления и национальной безопасности необходимо ввести обязательный курс по информационно-мировоззренческой безопасности, информационному противоборству и гибридным войнам.

1.5 Антикоррупционный механизм противодействия информационным угрозам в цифровой среде

Реализация государственной политики в сфере противодействия коррупции, основанной на предупреждении и борьбе с коррупцией и минимизации и (или) ликвидации последствий коррупционных правонарушений, предполагает не только постоянное совершенствование доктринального фундамента противодействия коррупции, но и своевременное выявление новых вызовов и угроз в данной сфере в целях выработки адекватных мер реагирования [137].

Задача эта обретает особую актуальность в современных условиях, ибо несмотря на активно предпринимаемые в этом направлении меры, количество коррупционных преступлений в Российской Федерации остается на неприемлемо высоком уровне; при оценке реального положения дел в этой сфере во внимание надо принимать также высокий уровень латентности преступлений в этой сфере. С этой точки зрения современные информационные технологии не только являются фактором, способствующим снижению коррупциогенных рисков, ибо позволяют уменьшить роль человеческого фактора в управлении, но и способны занять важное место в инструментарии противодействия коррупциогенным процессам.

Значение таких технологий в исследуемой области проявляется в нескольких направлениях. Первое проявляется в общем влиянии на государственно-политическую среду, выражающемся в том, что применение современных цифровых технологий в государственном управлении, обеспечивая информационную прозрачность деятельности государственных институтов, снижает уровень коррупциогенных рисков. Цифровые государственные услуги расширяют доступ к информации, прозрачность и подотчетность, повышая риск обнаружения коррупции и подрывая возможности ее осуществления.

Другое направление использования цифровых информационных технологий заключается в их применении в качестве специальных инструментов предупреждения и

противодействия коррупционным практикам посредством выявления, анализа, расследования, прогнозирования и мониторинга коррупционных нарушений; в данном случае речь идет о программных средствах, прямо предназначенных для решения конкретных задач в области противодействия коррупции. Так, технология ИИ позволяет значительно облегчить процесс выявления, анализа и прогнозирования коррупционных нарушений посредством ускорения обработки больших объемов данных, которая может оказаться слишком сложной и трудоемкой для сотрудников компетентных органов.

Большим потенциалом обладает программное выявление конфликта интересов посредством мониторинга поисковыми системами с использованием искусственного интеллекта. Через «виртуальные следы» в сети Интернет, поисковые запросы, сетевые сервисы, системы распознавания лиц, установления местонахождения, поиск одноклассников, родственные связи, финансовые транзакции с помощью специально разработанных программ можно отслеживать конфликты интересов и сигнализировать правоохранительным органам для проверки коррупционных схем.

Вместе с тем развитие новых технологий и цифровых решений способно продуцировать новые угрозы и уязвимости, в том числе коррупционной направленности [146]. Так, обеспечиваемая технологией блокчейн анонимность участников распределенного реестра предоставляет известные возможности для отмывания денег, мошенничества и киберпреступности. Однако сложность алгоритмов ИИ не позволяет точно сказать, как именно выполняется вычисление, приводящее к определенному результату, что неизбежно ведет к непрозрачности процесса, затруднению интерпретации причин принятия тех или иных решений ИИ и, как следствие, снижению доверия к программам, использующим ИИ.

Среди общих антикоррупционных механизмов следует выделить:

– совершенствование нормативно-правовой базы в области противодействий цифровой коррупции;
– создание институциональных механизмов;
– образование и повышение квалификации;
– использование инновационных технологий;
– контрольно-надзорные процедуры.

В связи с этим возможны следующие законодательные решения:

Необходимо законодательное закрепление понятия цифрового профиля как совокупности персональных данных, включающих предоставляемые данные, наблюдаемые данные, прогнозные данные, обработка которых осуществляется с использованием средств

автоматизации. В связи с этим необходимо внести изменения в законы о противодействии коррупции, о государственной гражданской службе в части установления ограничения в виде использования в отношении государственного служащего информационно-коммуникационных технологий анализа данных без его согласия (прохождения процедуры цифрового профилирования государственными служащими и должностными лицами в целях профилактики коррупционных и иных правонарушений).

Важным условием эффективной реализации механизмов предупреждения коррупции будет являться интеграция различных информационных систем (например, ГИС ТОР КНД, ЕФИР и др.) с ГИС «Посейдон» в части предоставления сведений о возможных коррупционных рисках, нарушениях ограничений, запретов и требований, установленных в целях противодействия коррупции со стороны должностных лиц. При этом в целях недопущения искажения предоставляемой информации, минимизации человеческого фактора необходимо предусмотреть автоматическую систему передачи сведений на основе срабатывания индикаторов коррупционных рисков.

Порядок использования цифрового профиля государственного служащего необходимо установить соответствующим Регламентом допуска уполномоченных представителей органов власти и отдельных организаций к цифровым профилям государственных служащих, а также Регламентом актуализации сведений, входящих в цифровой профиль.

2 Правовые механизмы обеспечения защищенности личности от информационных угроз в цифровой среде

2.1 Правовые формы и методы достижения защищенности личности от информационных угроз в цифровой среде

Необходимо учитывать, что столь стремительный рост цифровой мысли и темпы внедрения ее в различные направления абсолютно закономерно преумножают тот уровень угроз, с которыми может столкнуться или уже сталкивается человек и гражданин. Возникновение таких угроз непрерывно поднимает вопрос о противодействии угрозам человеку в информационной среде, методах борьбы с ними и их превенции. Информационная среда, в сегодняшнем ее понимании и представлении, неразрывно связана с цифровыми технологиями, информационной инфраструктурой и так далее, однако все же личность (человек) в ней занимает центральное место.

В целом же функционал государства обеспечен рядом правовых форм, позволяющих прямо или опосредовано влиять на правоотношения под своей юрисдикцией, коими и является информационное взаимодействие. В общем понимании речь идет о правотворческой, правоприменительной и управленческой, контрольно-надзорной деятельности.

Говоря о правотворческой форме обеспечения информационной безопасности в целом и безопасности личности в частности, необходимо упомянуть о том, что на характер правотворчества в данной сфере решающее воздействие оказывает особенность регулируемых правоотношений и их предмета. Так к первой категории предметов относится информация как таковая, то есть вся совокупность данных, сведений и сообщений, ресурсов. Вторая категория раскрывается через защиту прав субъектов информационных правоотношений, в том числе прав человека и гражданина. Третья категория опосредована защитой информационной инфраструктуры, то есть обеспечением свободного и безопасного доступа к данным, по существу, отнесенным к публичной информации.

В данном контексте государство, при совершенствовании правового регулирования должно учитывать право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, право на свободный доступ к информационным ресурсам, не отнесенным законом к ограниченным, право на свободный доступ к сети «Интернет» и обеспечение соответствующими технологиями.

В контексте правоприменительной и управленческой деятельности государства в данной сфере необходимо также отметить конституционную новеллу, где наряду с обороной и безопасностью относится к исключительному предмету ведения Федерации обеспечение информационной безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных. Данное положение указывает на то, что государственная политика в сфере информационной безопасности личности занимает отдельное место в структуре национальной безопасности, а деятельность органов государственной власти в этом направлении сопоставима по своему значению, например, с обороной государства от внешней военной угрозы. Также важно учитывать, что пресечение угрозы информационной безопасности, в том числе с преступной составляющей, в большинстве случаев возможно за счет управленческих действий, на этапе, когда такая угроза еще является потенциальной.

Иным аспектом правоприменительной и управленческой деятельности государства в сфере обеспечения информационной безопасности является борьба государства с информацией, которая составляет угрозу непосредственным воздействием на личность. В вопросах борьбы с «информационно-психологическими операциями» системные методы и

средства не сформированы. Одной из причин такого «пробела» служит характер информации и способ ее распространения. Основой деятельности правонарушителей является распространение неправдивой и вредоносной информации в сети «Интернет» с использованием общедоступных платформ обмена информацией таких как социальные сети, форумы, сервисы видеохостинга и прочее.

В данном случае борьба с таким явлением сопряжена с анализом большого количества информации и тотального контроля информационного публичного взаимодействия частных лиц. На сегодняшний день в Российской Федерации отсутствуют органы государственной власти, в том числе силовые структуры, которые имели бы целевую направленность, связанную с противодействием ИПсО («информационно-психологическая специальная операция»). Смежные отделы и департаменты существуют в Федеральной службе безопасности (Центр информационной безопасности ФСБ России), Министерстве внутренних дел (Управление по борьбе с киберпреступностью), а также в Министерстве обороны (войска информационных операций). Однако указанные организации и соединения имеют основную задачу, которую в общем можно охарактеризовать как защиту от противоправных действий в отношении государственной информационной инфраструктуры и расследование уже совершенных преступлений. Орган с функцией непосредственного противодействия дезинформации и информационного насилия над населением, по сведениям открытых и общедоступных источников, отсутствует.

Третьей формой обеспечения информационной безопасности личности является деятельность по государственному контролю (надзору) в сфере информации, информационных технологий и защиты информации. Сформирована и успешно осуществляет соответствующую деятельность Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Однако в ряде направлений деятельности компетенция службы лишь опосредованно затрагивает вопросы обеспечения информационной безопасности непосредственно личности.

Как результат изучения информационной безопасности личности и угроз, возникающих в связи с цифровой социализацией человека и гражданина, можно сделать следующие выводы:

1. Стремительное развитие технологий и технического прогресса, наряду с порождаемыми благами цифровой цивилизации, образует определенные угрозы, в первую очередь, для человека и гражданина (личности) как первичной и самой мало защищённой единицы общества.

2. Обеспечение информационной безопасности личности в основе своей проявляется через правотворческую, правоприменительную и управленческую и контрольно-надзорную деятельность государства.

3. Ориентиром правотворческой деятельности государства в данной сфере, ввиду ее специфичности, связанной с риском необоснованного притеснения частного интереса, должна служить задача вывести на первый план увеличение управленческих инструментов, направленных на профилактику рисков и купирование угроз, а не инструментов охранительной функции государства.

4. Правоприменение и управление должно исходить из задачи сформировать единую систему технологически оснащенных органов, чьей основной функцией будет не только защита государственной информационной инфраструктуры, но и, первостепенно, защита человека и гражданина от кибертеррора и информационно-психологического воздействия.

5. Контрольно-надзорная деятельность, используя риск-ориентированный подход, должна формироваться на основе защиты личности от рисков прежде, чем таковые становятся фактической реальностью, в частности, в вопросах обеспечения безопасности обработки персональных данных.

2.2 Обеспечение защищенности личности от информационных угроз в цифровой среде при формировании кадровой политики на государственной службе

Помимо организации взаимодействия органов государственной власти и местного самоуправления с гражданами, концепция цифрового государства предполагает решение вопросов интеграции цифровых и информационных технологий во внутреннюю организационную деятельность органов государственной власти и организацию государственной службы.

Цифровизация деятельности государственного аппарата как системы профессиональных кадров, обеспечивающих реализацию государственных функций, в определенной степени порождает угрозы, которые, в первую очередь, влияют на первичное звено – государственных служащих. При этом особенно важным аспектом является организация кадровой работы государственных служащих, в том числе борьба с угрозами, которые возникают в связи с цифровизацией государственного аппарата. К ним можно отнести, к примеру, защиту

персональных данных государственного служащего, цифровых прав государственных служащих, а также защиту государственного служащего от проявлений информационного терроризма, повышение уровня цифровой грамотности и пр.

В контексте исследования кадровой работы в сфере государственной службы в условиях цифровизации, в первую очередь, интересует, какие именно формы кадровой работы предполагают использование информационных и цифровых систем и технологий, чем в свою очередь образуют угрозы информационной безопасности личности. К таким формам работы можно отнести ведение трудовых книжек, реестра гражданских служащих, организация и проведение конкурсов на замещение вакантных должностей гражданской службы, формирование и организация работы кадрового резерва, обработка персональных данных государственных служащих.

Тем не менее наличие технических средств обеспечения информационной безопасности не гарантирует полного отсутствия угроз информационной безопасности личности при осуществлении кадровой работы в сфере государственной службы. Одной из таких угроз является ненадлежащая обработка и утечка персональных данных государственных служащих. Правовое регулирование правоотношений в сфере персональных данных госслужащего, в первую очередь, основывается на понимании того, что относится к таким данным и какое значение эта информация имеет для безопасности самого государственного служащего, поэтому правовой статус персональных данных государственного служащего и меры по защите этих данных, помимо технической обеспеченности кадровой работы органа должны исходить из необходимости полного нормативного обеспечения процесса получения и обработки персональных данных государственного служащего.

Вместе с тем в системе правового регулирования сформировался пробел, связанный с недостаточной регламентацией цифровых и информационных прав гражданского служащего, а также ограничений, связанных с прохождением службы. Существующих норм общего правового регулирования на уровне федерального законодательства, очевидно, недостаточно для того, чтобы сделать вывод о надлежащей реализации права гражданских служащих на свободный сбор и распространение информации и свободный доступ к информационным ресурсам.

Для разрешения сложившейся правовой проблемы, необходима доработка действующего законодательства. Федеральное законодательство должно быть дополнено нормой, определяющей четкие требования к публичному поведению государственного гражданского служащего в том числе с использованием ИТС «Интернет», нарушение которых будет

определяться в зависимости от обстоятельств, предусмотренных законом, дисциплинарным проступком, административным или уголовным правонарушением.

Также важным элементом обеспечения информационной безопасности личности при осуществлении кадровой работы в сфере государственной службы является повышение цифровой грамотности государственных гражданских служащих. Одним из решений ситуации видится внесение изменений в действующее законодательство. Персональным данным государственного служащего должен быть придан такой правовой режим, при котором ряд определенных законом сведений передается представителю нанимателя в обязательном порядке, а другие сведения (которые были упомянуты как необходимые для оценки виктимности) передаются государственным служащим добровольно в том объеме, в котором это необходимо для оценки уровня угрозы информационной безопасности.

Подводя итог, можно сформулировать ряд выводов.

Очевидно, что новые технологические веяния в сфере организации государственного управления неизбежно порождают угрозы цифровой безопасности личности и государства.

Государственные служащие, являясь фактически первичным звеном государственного управления, занимая должности, имеющие публично-правовое значение, наиболее подвержены таким угрозам.

Роль кадровой службы по обеспечению защищенности информационных прав государственного служащего проявляется в такой форме кадровой работы, как консультирование гражданских служащих по правовым и иным вопросам гражданской службы, поскольку ряд аспектов ограничения информационных прав в связи с прохождением государственной службы еще в должной мере не урегулирован.

Действующее правовое регулирование обработки персональных данных государственных служащих имеет ряд недостатков и несоответствий. К таким недостаткам, в первую очередь, необходимо отнести недостаточное правовое урегулирование вопроса о понятии персональных данных государственного служащего и об исчерпывающем перечне предоставляемых государственным служащим персональных данных, сведениях, о порядке их передаче третьим лицам, в том числе в средства массовой информации и т.д.

2.3 Ответственность в области защищенности личности от информационных угроз в цифровой среде

В контексте исследования защищенности личности от информационных угроз, ее роль в реализации данного принципа, который полностью применим ко всем современным цивилизованным правопорядкам, сводится к тому, что меры по защите информации призваны

обеспечить, с одной стороны, реализацию права на доступ к информации, с другой – соблюдение конфиденциальности информации ограниченного доступа. В свою очередь государственное регулирование отношений в сфере защищенности личности от информационных угроз выражается в установлении требований по защите информации, во введении ответственности за нарушение законодательства Российской Федерации, которые в полной мере соответствуют требованиям правового государства и современным вызовам демократического развития.

Спецификация информационных угроз в цифровой среде позволила с определенной долей условности выделить деяния, которые можно разделить на три блока: разглашение, утечка, несанкционированный доступ. За нарушение требований Закона о информации предусмотрена дисциплинарная, гражданско-правовая, административная или уголовная ответственность в соответствии с законодательством Российской Федерации.

Дисциплинарная ответственность. Законодательно не определен особый порядок привлечения к дисциплинарной ответственности за проступки, посягающие на права личности в цифровой среде, однако анализ судебной практики и статистические данные позволяют сделать вывод, что большая часть деликтов, совершаемых в данной сфере связана с действиями направленными на утечку информации ограниченного доступа и обусловлена ненадлежащим исполнением работником его обязанностей. В основном к дисциплинарной ответственности в информационной сфере привлекаются за разглашение персональных данных через различные мессенджеры, если в действиях лица отсутствуют признаки состава административного или уголовно наказуемого деяния. Здесь, следует заметить, что в отдельных случаях деяние лица может одновременно содержать и признаки дисциплинарного проступка, административного правонарушения и преступления.

Административная ответственность в области защищенности личности от информационных угроз в цифровой среде устанавливается КоАП РФ, а также законами субъектов РВ, в пределах, установленных федеральным законодательством. Основной массив составов административных правонарушений сосредоточен в главе 13 «Административные правонарушения в области связи и информации».

По сравнению с административными правонарушениями преступления отличаются наибольшей степенью общественной опасности. Определяя контуры защищенности личности от информационных угроз в цифровой среде посредством уголовной ответственности, необходимо отметить, что стремительное развитие информационных технологий является предпосылкой для образования новых форм преступности.

В отличие от ранее рассмотренных публично-правовых видов отраслевой ответственности, гражданская ответственность направлена на реализацию правовосстановительной функции. Общей формой деликтной ответственности является возмещение вреда. Вытекающее из правовосстановительной функции правило о полном возмещении вреда направлено на устранение всех негативных последствий нарушения субъективного права и выражается в праве потерпевшего требовать возмещения реального ущерба и упущенной выгоды.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило решить ряд крупных теоретических и прикладных задач. В рамках исследования вопросов правового обеспечения защищенности личности от информационных угроз в цифровой среде прежде всего предложены правовые конструкции, направленные на развитие комплексного правового регулирования и правоприменительной практики в области защищенности личности от информационных угроз в цифровой среде в системе концептуально-ценностного, программного и нормативного регулирования в области информационной безопасности и национальной безопасности. Выявлена необходимость формирования национальной модели цифровизации и цифровой безопасности, определяющей направления совершенствования организационно-правовой основы информационной безопасности в контексте идеалов и принципов прав человека.

Научная оценка и анализ тенденций и перспектив развития законодательства в данной области позволили высказать предложения прикладного характера, направленные на разработку правового механизма противодействия негативному информационному воздействию и информационному насилию, в том числе, путем усиления ответственности за правонарушения в цифровой среде и с использованием цифровых технологий; разработку правового механизма независимой экспертизы и независимого аудита в области цифровых технологий; совершенствование мер идентификации и аутентификации в целях решения вопроса минимизации утечек персональных данных является; запрет ограничение личного цифрового суверенитета.

Анализ и оценка концепции информационно-мировоззренческой безопасности позволили определить данный социальный инструмент как самостоятельный правовой институт, систематизация которого возможна только в порядке принятия специального федерального закона, что будет являться следствием принятия Доктрины мировоззренческой безопасности. В предлагаемом законодательном акте следует среди прочего закрепить

правовые основы: системы прогнозирования, выявления и предупреждения информационно-мировоззренческих угроз, определения их источников, ликвидации последствий реализации таких угроз; взаимодействия между уполномоченными органами исполнительной власти по предотвращению деструктивного информационно-мировоззренческого воздействия, повышению защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования; основания и пределы делегирования соответствующих полномочий органам публичной власти субъектов Российской Федерации и органам местного самоуправления; системы организационно-правовых форм и методов обеспечения информационно-мировоззренческой безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления; сотрудничества Российской Федерации с дружественными странами в области обеспечения информационно-мировоззренческой безопасности; подготовки кадров в области информационно-мировоззренческой безопасности, информационного противоборства и гибридных войн.

Авторы считают, что разработанные ими идеи и теоретические положения окажут серьезное влияние на совершенствование законодательства России в области правового обеспечения информационной безопасности, а также будут способствовать развитию эффективной модели защищенности личности от информационных угроз в цифровой среде с учетом современных вызовов и угроз, положительным тенденциям развития национальной правовой системы и публичного управления.

Благодарности: Материал подготовлен в рамках выполнения научно-исследовательской работы государственного задания РАНХиГС.

СПИСОК ИСТОЧНИКОВ

1. Указ Президента РФ от 23.11.2020 № 733 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации на период до 2030 года» – URL: http://pravo.gov.ru (дата обращения: 10.05.2023)

2. Указ Президента РФ от 29.05.2020 № 344 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации до 2025 года» – URL: http://www.pravo.gov.ru (дата обращения: 10.05.2023).

3. Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года (разработан Минэкономразвития России) – URL: http://www.economy.gov.ru (дата обращения: 10.05.2023).

4. Распоряжение Правительства РФ от 31.12.2020 № 3684-р «Об утверждении Программы фундаментальных научных исследований в Российской Федерации на долгосрочный период (2021 - 2030 годы)» (ред. от 21.04.2022)// Собрание законодательства Российской Федерации. 2021. № 3. Ст. 60.

5. Противодействие коррупции: новые вызовы: монография / отв. ред. Т.Я. Хабриева. – М., 2016.

6. Новые технологии для устойчивого развития: перспективы использования для обеспечения добросовестности, доверия и борьбы с коррупцией» (New Technologies for Sustainable Development: Perspectives on Integrity, Trust and Anti-Corruption). Доклад об использовании новых технологий в борьбе с коррупцией Программы развития ООН (United Nations Development Programme – UNDP). – URL: https://anticor.hse.ru/main/news_page/opublikovan_doklad_ob_ispolzovanii_novyh_tehnologiy_v_borbe_s_korruptsiey (дата обращения: 29.05.2023).

В СЕРИИ ПРЕПРИНТОВ РАНХиГС РАССМАТРИВАЮТСЯ ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ ПОДХОДЫ К СОЗДАНИЮ, АКТИВНОМУ ИСПОЛЬЗОВАНИЮ ВОЗМОЖНОСТЕЙ ИННОВАЦИЙ В РАЗЛИЧНЫХ СФЕРАХ ЭКОНОМИКИ КАК КЛЮЧЕВОГО УСЛОВИЯ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ

РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ