МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

40.05.01 Правовое обеспечение национальной безопасности
(код и наименование направления подготовки / специальности)

Государственно-правовая
(направленность (профиль) / специализация)

# ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему: «Государственно-правовой механизм обеспечения информационной безопасности»

Обучающийся Е.Н. Поршнев
(Инициалы Фамилия) (личная подпись)

Руководитель д.ю.н., профессор, Д.А. Липинский
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

## Аннотация

До провозглашения на конституционном уровне права на информацию, данный вопрос был предметом многочисленных научных обсуждений. Основной вопрос, который ставился – это вопрос о том, что каждый имеет право на информацию. Данное право в Российской Федерации закреплено в действующей Конституции РФ (ст. 29), которое признается важным атрибутом гражданского общества.

Наличие проблемы обеспечения информационной безопасности и ее недостаточное нормативное правовое регулирование делает настоящую работу актуальной.

Объектом исследования - общественные отношения в информационной сфере.

Предмет исследования - нормы действующего законодательства, регулирующие, направленные на регулирование информационной безопасности в Российской Федерации, исследования ученых в данной области общественны отношений.

Цель выпускной квалификационной работы – провести научно-правовой анализ государственно-правового механизма, обеспечивающего информационную безопасность Российской Федерации.

**Оглавление**

# Введение

Актуальность темы исследования. До провозглашения на конституционном уровне права на информацию, данный вопрос был предметом многочисленных научных обсуждений. Основной вопрос, который ставился – это вопрос о том, что каждый имеет право на информацию. Данное право в Российской Федерации закреплено в действующей Конституции РФ [32] (ст. 29), которое признается важным атрибутом гражданского общества [55].

Следует согласиться с тем, что информатизация общества привнесла много положительного. В частности, деятельность государственных структур стала более открытой. Информационные технологические системы становятся одним из приоритетов повышения эффективности взаимодействия государства и общества, особенно при решении государственных задач и разработке программ и стратегий развития государства. Эффективная реализация государственного управления требует разработки моделей, способных к объединению различных методик, механизмов и инструментов, специализированных экономических и отраслевых областей знаний, адаптированных к государственному управлению.

В последние два десятилетия одним из приоритетных направлений российской государственной политики стало развитие информационного обеспечения деятельности органов государственной власти, в частности, государственных органов исполнительной власти. При этом одним из компонентов, который показывает уровень прозрачности в государстве, является информационная открытость органов государственной власти. Раскрытие данных повышает прозрачность и подотчетность в деятельности этих органов, способствует более эффективному использованию государственных ресурсов, улучшает качество государственных услуг, а также способствует развитию инновационного бизнеса и созданию общественно полезных услуг. На основе открытых данных рассчитывается

индекс конкурентоспособности стран мира в глобальном экономическом рейтинге (так, в Рейтинге стран мира по уровню глобальной конкурентоспособности в 2021 г Россия заняла 45 место по уровню конкурентоспособности (поднявшись с 50 места в 2020 году) [99]).

Счетная палата РФ совместно с АНО «Информационная культура» и Центром перспективных управленческих решений в экспертном докладе «Открытость государства в России-2020» составила рейтинг федеральных органов исполнительной власти в 2020 году по уровню открытости, в котором только одно министерство получило оценку «высокая открытость» (Министерство энергетики), еще 9 министерств получили оценку «средний уровень открытости», а открытость 11 министерств была оценена как низкая [40].

В рейтинге открытости 2021 г., составленного в отношении служб, агентств и управлений, только два государственных органа получили оценку «высокий уровень открытости» (Росмолодежь, Федеральная служба судебных приставов), еще 20 органов получили оценку «средний уровень открытости», а 29 – оценку «низкий уровень открытости. Основные претензии проверяющих органов касались взаимодействия государственных органов исполнительной власти взаимодействия с гражданами. Эффективность информационного обеспечения деятельности органов исполнительной власти и прозрачности управленческих процессов в настоящее время развивается.

В тоже время, закрепив право на информацию в ст. 29 Конституции РФ, возникла проблема защиты от информации [1]. Развитие и внедрение информационных технологий оказывают возрастающее влияние на все стороны жизни государства и общества. Вместе с тем по мере развития этой базы повышается и уязвимость информационного пространства.

Современное общество находится в состоянии активной трансформации сферы коммуникации. Практически не осталось общественных отношений, которые не были бы опосредованы цифровыми технологиями. При всей перспективности развития новых видов коммуникации некоторые вопросы остаются, как минимум, дискуссионными.

Исследователи выражают обеспокоенность наличием деструктивного информационно-психологического влияния на несовершеннолетних, которое приводит к появлению у них состояния психического напряжения, внутреннего дискомфорта, угнетенного чувства безопасности [13].

По подсчетам специалистов более половины граждан сегодня считают, что Интернет, наряду с позитивными результатами, способен стать для них информационной угрозой [54]. В связи с этим особую актуальность приобретает проблема защиты права личности, общества и государства на конфиденциальность, на свободу от деструктивного воздействия медиапространства [27].

С другой стороны, трудно не согласиться со слабой проработанностью опросов правового регулирования обеспечения информационной безопасности в Интернете. «В России на данный момент – пишет Ю.П. Калиниченко – существует свободная система и достаточно либеральная модель регулирования Интернета. В частности, отсутствуют какие-либо серьезные ограничения на поток информации в Сети, нет цензуры в отношении интернет-транзакций, что, конечно, отличается от ситуации с телевидением или радиовещанием. В России Интернет остается зоной свободных коммуникаций» [27, с. 89].

Как отмечает В.Н. Верютин, «необходимо понимать, что угрозы информационной безопасности в настоящее время носят не абстрактный характер, каждой из них соответствуют целенаправленные действия конкретных носителей враждебных намерений. В результате таких деяний может быть нанесен урон жизненно важным интересам государства, обществу или отдельным гражданам» [12, с. 138].

Таким образом, наличие проблемы обеспечения информационной безопасности и ее недостаточное нормативное правовое регулирование делает настоящую работу актуальной.

Объектом исследования - общественные отношения в информационной сфере.

Предмет исследования - нормы действующего законодательства, регулирующие, направленные на регулирование информационной безопасности в Российской Федерации, исследования ученых в данной области общественны отношений.

Цель выпускной квалификационной работы – провести научно-правовой анализ государственно-правового механизма, обеспечивающего информационную безопасность Российской Федерации.

Задачи исследования:

- провести теоретико-правовой анализ понятия информационной безопасности и основных ее угроз;
- рассмотреть нормативно-правовые основы обеспечения информационной безопасности;
- проанализировать государственные органы, органы местного самоуправления, уполномоченных на обеспечение информационной безопасности;
- выявить вопросы, возникающие при обеспечения информационной безопасности в деятельности органов государственной власти;
- отдельное внимание уделить организационно-правовым основам обеспечения информационной безопасности в сфере образования и воспитания;
- наметить основные направления обеспечения информационной безопасности в сфере образования и воспитания.

Нормативно-правовая база исследования представлена Конституцией РФ, нормами федерального и регионального законодательства в части обеспечения информационной безопасности.

Теоретическая основа представлена трудами следующих ученых: С.А. Авакьяна, А.И. Алексенцевой, А.В. Андреевой, А.В Баркова, И.Л.Бачило, Э.М. Брандман, В.Н. Верютина, Л.А. Гаязовой, Е.В. Дороговой, А.Д. Желонкина, А.М. Иванцова, Ю.П. Калинченко, А.В. Крутских, Н.Н. Пономарева и др.

Структура выпускной квалификационной работы предопределена поставленной целью и задачами исследования и включает: введение, три главы, шесть параграфов, заключение и список используемой литературы и используемых источников.

# Глава 1 Общая характеристика обеспечения национальной безопасности Российской Федерации в информационной сфере

## 1.1 Понятие информационной безопасности и анализ информационных угроз

Информационная безопасность является частью национальной безопасности, под которой понимается «состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны» (пп. 1 п. 5 Стратегии национальной безопасности Российской Федерации [74]).

Информационная безопасность в п. 26 рассматриваемой Стратегии указана как один из стратегических национальных приоритетов, направленных на защиту национальных интересов РФ, целью обеспечения которой является укрепление суверенитета Российской Федерации в информационном пространстве (п. 56 Стратегии национальной безопасности).

Непосредственно понятие информационной безопасности сформулировано в действующей Доктрине информационной безопасности Российской Федерации [76] «как защищенность личности, общества и государства от информационных угроз извне и изнутри, обеспечивающее реализацию конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое социально-экономическое развитие Российской Федерации, оборону и безопасность государства».

Несмотря на существующее легальное определение информационной безопасности, данная дефиниция рассматривается и в научно-теоретическом аспекте.

К примеру, по мнению А.И. Алексенцева информационная безопасность – это «состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиты субъектов от негативного информационного воздействия» [3, с. 45].

Можно встретить понимание информационной безопасности как защиты от информации. Например, С.П. Расторгуев, считает, что «в результате проблема защиты информации, которая ранее была как никогда актуальна, перевернулась подобно монете, что вызвало к жизни ее противоположность. Теперь уже саму информационную систему и, в первую очередь человека - необходимо защищать от поступающей «на вход» информации, потому что любая поступающая на вход самообучающейся системы информация неизбежно изменяет систему. Целенаправленное же деструктивное информационное воздействие может привести систему к необратимым изменениям и, при определенных условиях, к самоуничтожению» [59, с. 47].

Понятие «информационная безопасность» достаточно тесно взаимосвязано с понятием «безопасность информации» или «защита информации», они достаточно синонимичны. Но «безопасность» не может существовать сама по себе, безотносительно к объекту, «без внутреннего смысла» [67, с. 55].

Таким образом, информационная безопасность является широким понятием, включающее в себя все, что взаимодействует с информацией.

В настоящее время можно выделить некоторые виды информационной безопасности, в частности международной. По данному вопросу Президентом РФ утверждены Основ государственной политики Российской Федерации в области международной информационной безопасности [83]. В данных Основах под международной информационной безопасностью понимается

«такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности».

А.В. Крутских и Е.С. Зиновьева считают, что приведенный в Основах термин «международная информационная безопасность» подразумевает наличие не только технических, но и политико-идеологических угроз в данной области [34, с. 6].

С.Е. Смирных, признает международную информационную безопасность как одну из гарантий осуществления права народов на самоопределение [64].

В виду того, что информационная безопасность – это комплекс мер по обеспечению защиты информации, отдельного внимания заслуживает рассмотрение понятия «защита информации». Под таковой понимают совокупность действий по предотвращению утечки, хищения, утраты, подделки, несанкционированных и непреднамеренных воздействий на определенную информацию.

Ключевые принципы информационной защиты:

- конфиденциальность;
- целостность информации;
- доступность информации;
- целостность;
- невозможность отказа.

Исходя из вышесказанного, можно выделить следующие цели защиты и информации:

- предотвращение утечки информации;
- обеспечение безопасности и конфиденциальности;
- защита конституционных прав граждан на сохранение личной тайны конфиденциальности персональных данных;

– сохранение возможности управления процессом обработки и пользования информацией без посторонних вторжений.

Информационная безопасность, как сфера занятости, значительно расширилась и в ней возникли новые профессии, такие как специалист по обеспечению безопасности сетей и связанной инфраструктуры, защиты программного обеспечения и баз данных, аудитор информационных систем, планировщик непрерывности бизнеса.

Исходя из принципов системного подхода защита информации должна обладать следующими критериями:

– непрерывность – ценная информация должна быть защищена в любом массиве системы;
– систематизированность – защита должна представлять систему, охватывающую особо важную информацию;
– целенаправленность и конкретность – защищаться должна та информация, которая наиболее важна для организации;
– активность – методы защиты информации должны постоянно модернизироваться, исходя из современных возможностей хакерства;
– надежность – информация должна быть защищена вне зависимости от объема и формата;
– универсальность – комплекс мер по защите информации должен обеспечить информацию от всевозможных видов угроз;
– комплексность – для защиты информации должны применяться все виды и формы защиты в полном объеме.

Теория защиты информации – система знаний о защите информации в современных системах, раскрывающая в полной мере представление о сущности проблемы защиты, Данная теория развивается на основе опыта практического решения задач защиты [65, с. 83].

В Доктрине информационной безопасности выделены угрозы информационной безопасности.

Как отмечает В.Н. Верютин, «необходимо понимать, что угрозы информационной безопасности в настоящее время носят не абстрактный характер, каждой из них соответствуют целенаправленные действия конкретных носителей враждебных намерений. В результате таких деяний может быть нанесен урон жизненно важным интересам государства, обществу или отдельным гражданам» [12, с. 138].

Очевидно, что интересы личности, общества и государства в вопросах информационной безопасности должны быть признаны взаимными и нуждающимися в обеспечении безопасности. Но проблема заключается как раз в неоднозначности общественной (и неполноте правовой) оценки как самих угроз информационной безопасности, так и возможных негативных последствий их воздействия. Можно согласиться с Н.Р. Шевко, который считает, что «правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных систем. Угрозы информационной безопасности – это оборотная сторона использования информационных технологий» [95, с. 59].

А.Н. Привалов и Ю.И. Богатырева обращают внимание на то, что «угрозы могут быть как реальными, т.е. уже проявившимися в своем негативном, разрушительном воздействии на объект безопасности, так и потенциальными, т.е. их негативное воздействие может проявить себя в ближайшем или отдаленном будущем» [51, с. 428].

В контексте рассматриваемой проблемы важным представляется то, что под угрозой принято понимать потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам [51, с. 428]. То есть для определения меры ответственности за нарушения в сфере информационной безопасности необходимо представлять степень неблагоприятных последствий для личности, общества и государства,

которые могут возникнуть в случае реализации угрозы. В данном аспекте важно рассмотреть понятие «вредной информации».

Так, И.Л. Бачило трактует этот термин как информацию, распространение или применение которой влечет необходимость защиты субъектов информационных правоотношений от ее негативного воздействия [8, с. 342].

В.А. Копылов считает, что воздействие вредной и опасной информации может привести к нарушению информационных прав и свобод, дестабилизации общества, нарушению стабильности и целостности государства [33, с. 240].

Политико-правовой аспект данной проблемы заключается в том, что, как справедливо отмечает И.И. Тазин, «всякий раз решение вопроса об отнесении того или иного вида информации к категории деструктивной находит противодействие со стороны средств массовой информации в виде абсолютизированного понимания конституционно-правового запрета на цензуру» [69, с. 223].

Обоснованной представляется точка зрения И.И. Тазина, по мнению которого, «в действительности же положение ч. 5 ст. 29 Конституции РФ о свободе массовой информации и запрете цензуры необходимо рассматривать в связке с ч. 3 ст. 56 Конституции РФ, в соответствии с которой права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (соответствующей ст. 10 Европейской конвенции о защите прав человека и основных свобод), а также во взаимосвязи со ст. 3 ФЗ «О средствах массовой информации» [22] о запрете предварительной цензуры, ст. 4 ФЗ «О средствах массовой информации» о недопустимости злоупотребления массовой информацией. Следовательно, установление видов юридической ответственности за распространение деструктивной информации является

мерой ответственности за злоупотребление свободой информации в целях защиты здоровья и нравственности населения. Деятельность контрольно-надзорных, правоохранительных органов и общественных организаций по выявлению источников деструктивной информации и привлечению к ответственности виновных лиц не может рассматриваться как цензура, поскольку эта деятельность не связана с предварительным согласованием информационной продукции с должностными лицами, государственными органами или организациями. Из сопоставления указанных правовых норм следует, что средства массовой информации свободны и их продукты не подлежат предварительной цензуре до выхода в свет. В случае если выпущенная информационная продукция переходит черту, обозначенную ч. 3 ст. 56 Конституции РФ, и подпадает под признаки деструктивной информации, создавая угрозу личности, обществу и государству, необходимы меры государственного и общественного реагирования» [69, с. 223]. Солидарен с автором и К.Д. Рыдченко [60, с. 41].

Следует, согласиться также с точкой зрения И.И. Тазина относительно злоупотребления свободой массовой информации в форме распространения деструктивной информации, которая, подлежит криминализации, поскольку деструктивные программы насилия, жестокости и саморазрушения посягают на общественные отношения, обеспечивающие безопасность жизни и здоровья человека [69, с. 223].

Во времена, когда компьютерные технологии стремительно развиваются, защита информации является важным аспектом, как в работе крупных компаний, так и при работе с личными данными. Но риски и угрозы информационной безопасности, и их осуществление так же развивается с каждым днем.

Итак, угроза информационной безопасности – это попытка осуществить неблагоприятные воздействия на объект информационной среды, воздействуя на его информационные ресурсы, технологии и технические средства обработки и передачи информации.

Источники информационной безопасности бывают двух видов – внутренние и внешние.

Внутренние:

- противозаконная деятельность различных структур, лиц, групп в сфере информации;
- неправомерное регулирование правовых отношений в информационной среде;
- нарушение или невыполнение, установленных регламентом сбора, обработки и передачи информации;
- ошибки персонала и пользователей, непреднамеренные и преднамеренные ошибки разработчиков, пользователей;
- недостаточно современное развитие информационной среды;
- отказы и сбои технических систем.

Внешние:

- политика иностранных государств;
- действия разведок и спецслужб;
- экспансия информационных систем в другие государства;
- противозаконная деятельность преступных групп;
- стихийные бедствия и природные катаклизмы.

Захват информации осуществляется путем несанкционированного захвата информации. Рассмотрим некоторые пути захвата.

- косвенным – без физического доступа к элементам локальных сетей;
- прямым – непосредственно с физическим доступом к элементам локальных сетей.

Риск информационной безопасности – возможность нарушения информационной безопасности с негативными последствиями. Основными рисками информационной безопасности являются:

- риск утечки конфиденциальной информации;
- риск потери или недоступности важных данных;

– риск использования неполной или деформированной информации;
– риск неправомочной скрытой эксплуатации информационно-вычислительных ресурсов (например, при создании бот-сети);
– риск распространения во внешней среде информации, угрожающей репутации организации.

Уязвимость информационной системы – недостаток в системном или прикладном программном обеспечении, который может использоваться для реализации угрозы безопасности информации.

Причины возникновения уязвимостей:

– ошибки или недоработки при проектировании и разработке обеспечения;
– преднамеренные действия по внесению уязвимостей в ходе проектирования системы;
– неправильные настройки программного обеспечения;
– использование вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
– случайные неумышленные действия пользователей, приводящие к возникновению уязвимостей;
– сбои в работе аппаратного и программного обеспечения [65, с. 88].

Атаки на систему – действия, использующие уязвимости информационной системы и приводящие к нарушению доступности, целостности и конфиденциальности обрабатываемой информации. Последствия атак велики: финансовые убытки, распространение личных данных, распространение разработок, потеря клиентов и т.д.

Способы осуществления угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации

Искажение информации – намеренная или случайная передача неполной истинной информации. Существуют следующие виды искажения информации:

– обман или дезинформация;

– двусмысленность высказывания;
– неполнота информации;
– шифровка информации.

Каналы искажения информации: электромагнитный канал, акустический канал, визуальный канал, информационный канал, который может быть разделен на следующие каналы:

– коммутируемых линий связи;
– выделенных линий связи;
– локальной сети;
– машинных носителей информации;
– терминальных и периферийных устройств.

Можно выделить следующие причины искажения информации:

– ошибки, вносимые оконечными комплектами аппаратуры передачи данных;
– искажения, вносимые каналом: шум канала, частотные искажения, потери информации по причине временной неработоспособности.

Методы нарушения конфиденциальности, целостности и доступности информации: подслушивание, перехват информации и установление в аппаратуру или изменение программ, содержащихся в ПЗУ компьютерной системы, программных или технических средств, которые нарушают ее структуру и функции.

Политика безопасности – это совокупность норм и правил, определяющих принятые в организации меры по обеспечению безопасности информации, связанной с деятельностью организации.

Информационные риски – угроза безопасности информации. Бывают следующих видов:

– риски, связанные с информационной безопасностью
– риски качества управления информационными услугами
– проектные риски.

Управление информационными рисками организуется в соответствии с политикой управления информационными рисками предприятия.

Качественный анализ риска определяет факторы риска, этапы работы, при выполнении которых риск возникает.

Количественная оценка риска – это численное определение влияния отдельных рисков проекта.

В целом, можно выделить следующие проблемы информационной безопасности.

Во-первых, это проблемы гуманитарного характера, возникающие в связи с бесконтрольным использованием и распространением персональных данных, вторжениями в частную жизнь, клеветой и др. относительно конкретной личности.

Во-вторых, проблемы экономического и юридического характера, возникающие в результате утечки, искажения и потери защищаемой информации.

В-третьих, проблемы политического характера, возникающие из-за информационных войн [24, с. 25].

Изложенное позволяет сделать вывод о том, что информационная безопасность является составной частью системы национальной безопасности Российской Федерации и представляется состояние определенного объекта и деятельность, направленную на организацию обеспечения состояния защищенности данного объекта.

Угроза безопасности информации – это потенциальная возможность нарушения основных качественных характеристик (свойств) информации: конфиденциальности, целостности и доступности – при ее обработке техническими средствами. Таким образом, понятие «угроза» заключается в образовании каких-либо обстоятельств, условий, процессов, влияющих на информацию, имеющую определенную сущность. Угроза информации может возникнуть по вполне определенным причинам (факторам). Как известно, слово «фактор» происходит от латинского factor («делающий»,

«производящий») и обозначает движущую силу, причину какого-либо процесса, явления. Множество факторов опасности (причин возникновения угроз) можно свести в три основных группы:

- природные факторы, вызываемые физическими воздействиями стихийных природных явлений (наводнения, землетрясения, магнитные бури, радиоактивные излучения и т.д.). Названные факторы в большинстве случаев неявно зависят или вообще не зависят от деятельности человека;
- технические факторы, вызываемые сопутствующими работе радиоэлектронной аппаратуры побочными электромагнитными излучениями и их наводками на окружающие металлические предметы, ошибками в проектировании, в программном обеспечении, случайными сбоями в работе ПЭВМ и линий связи, энергопитания, воздействием на аппаратуру физических полей при несоблюдении условий электромагнитной совместимости и т.д. Эти факторы опосредованно зависят от деятельности человека, хотя сбои в работе оборудования и пропадания энергопитания могут быть вызваны целенаправленно;
- социальные факторы, обусловленные происходящими в обществе экономическими, политическими, нравственными изменениями и проявляющиеся в виде ошибок пользователей, несанкционированных действий обслуживающего персонала и несанкционированного воздействия на ресурсы информационных систем как со стороны своих сотрудников (внутренний нарушитель), так и посторонними лицами (внешний нарушитель), либо теми и другими, действующими в сговоре. Данные факторы непосредственно зависят от деятельности человека.

## 1.2 Нормативно-правовые основы обеспечения информационной безопасности

Нормативно-правовые основы обеспечения информационной безопасности можно разделить на документы концептуального уровня, федеральное законодательства и другие нормативно-правовые акты.

К документам концептуального уровня относится, прежде всего, Конституция Российской Федерации, провозгласившая:

- право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23 Конституции РФ);
- запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия (ст. 24 Конституции РФ);
- право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29 Конституции РФ);
- перечень сведений, составляющих государственную тайну, определяется федеральным законом (ст. 29 Конституции РФ);
- органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

К концептуальным документам относится Доктрина информационной безопасности, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. В Доктрине вводится понятие «информационной сферы», изложены национальные интересы в информационной сфере,

основные информационные угрозы и состояние информационной безопасности и организационные основы ее обеспечения.

Как уже отмечалось выше, в 2021 году Президент РФ утвердил Основы государственной политики Российской Федерации в области международной информационной безопасности. Названный документ являются документом стратегического планирования Российской Федерации и отражают официальные взгляды на сущность международной информационной безопасности, определяют основные угрозы международной информационной безопасности, цель, задачи государственной политики Российской Федерации в области международной информационной безопасности (далее - государственная политика в области международной информационной безопасности), а также основные направления ее реализации.

В Основах государственной политики в области международной безопасности сущность международной информационной безопасности, основные угрозы, цель и задачи государственной политики в области международной информационной безопасности. Так, целью государственной политики в области международной информационной безопасности является содействие установлению международно-правового режима, при котором создаются условия для предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве, а также для формирования с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности.

Кроме того, в Основах государственной политики в области международной безопасности обозначены основные направления реализации государственной политики и механизмы ее реализации.

Среди федеральных законов, составляющих правовую основу обеспечения информационной безопасности, можно назвать следующие:

– Федеральный закон «О безопасности» [90], определяющий основные принципы и содержание деятельности по обеспечению безопасности

государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации;

- Федеральный закон «Об информации, информационных технологиях и защите информации» [88], регулирующий отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, применении информационных технологий и обеспечении защиты информации;
- Федеральные законы, регулирующие особенности доступа к информации о деятельности отдельных органов государственной власти [86]; [87];
- Федеральный закон «О государственной тайне» [21], согласно которому государственная тайна особо охраняется государством и представляет собой «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации»;
- Федеральный закон «О персональных данных» [89], целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- Закон «О средствах массовой информации» отображает основные понятия СМИ, организация их деятельности, а также порядок распространения информации и ответственность за нарушение

законодательства о средствах массовой информации. Данным законом охраняется право на неприемлемость цензуры и четко прописаны моменты, когда не допускается массовое использование информации.

Вся система обеспечения информационной безопасности не в состоянии эффективно работать в ситуации, когда отсутствуют механизмы привлечения к ответственности за нарушение установленных норм и правил, либо за различные деструктивные воздействия на механизмы системы. Ответственность за нарушения в сфере обеспечения информационной безопасности определяются положениями Гражданского кодекса Российской Федерации [15] в части возмещения вреда, Уголовный кодекс Российской Федерации [71] и Кодекса РФ об административных правонарушениях (далее – КоАП РФ) [30] в части административной ответственности за правонарушения, посягающие на отношения в сфере информационной безопасности (в широком смысле).

Важное значение для обеспечения информационной безопасности имеют Указы Президента РФ, помимо приведенных выше, имеющих стратегическое и концептуальное значение.

Так, Указ Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [73] поручает Правительству определить перечень ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России.

Во исполнение данного Указа Правительство РФ утвердило перечень из 72 субъектов, которые до 1 июля должны представить правительству доклады об уровне защищенности своих информационных систем [56].

В частности, это потребуется сделать:

- ряду федеральных ведомств, в числе которых Минфин и ФНС;
- правительствам Москвы и Санкт-Петербурга;

– нескольким банкам;

– некоторым авиакомпаниям.

Кроме того, Указ Президента РФ «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» предусматривает проведение мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак, предполагая в долгосрочной перспективе отказаться от зарубежного компьютерного оборудования и программного обеспечения [7].

Указами Президента РФ регулируются отдельные направления, связанные с защитой отдельных видов информации [77]; [75].

Нормативными актами Правительства РФ регулируются конкретные направления информационной безопасности [45], осуществляется оперативное реагирование на вновь возникающие угрозы в сфере информационной безопасности [46].

В целом, на уровне подзаконного нормотворчества развиваются и конкретизируются отдельные направления регулирования информационной безопасности. Дальнейшая конкретизация отдельных правовых механизмов, регулирующих отношения в сфере информационной безопасности, осуществляется на уровне приказов отдельных федеральных органов исполнительной власти.

Выводы по первой главе выпускной квалификационной работы.

Во-первых, информационная безопасность является составной частью системы национальной безопасности Российской Федерации и представляется состояние определенного объекта и деятельность, направленную на организацию обеспечения состояния защищенности данного объекта. Угроза безопасности информации – это потенциальная возможность нарушения основных качественных характеристик (свойств) информации: конфиденциальности, целостности и доступности – при ее обработке техническими средствами. Таким образом, понятие «угроза» заключается в образовании каких-либо обстоятельств, условий, процессов, влияющих на

информацию, имеющую определенную сущность. Угроза информации может возникнуть по вполне определенным причинам (факторам).

Во-вторых, нормативно-правовые основы обеспечения информационной безопасности можно разделить на документы концептуального уровня, федеральное законодательства и другие нормативно-правовые акты. К документам концептуального уровня относится, прежде всего, Конституция Российской Федерации, Доктрина информационной безопасности, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Важное значение для обеспечения информационной безопасности имеют федеральные законы, а также указы Президента РФ, помимо, приведенных выше, имеющих стратегическое и концептуальное значение.

# Глава 2 Организационно-правовой механизм обеспечения информационной безопасности

## 2.1 Государственные органы, органы местного самоуправления и их должностные лица, уполномоченные на обеспечение информационной безопасности

Организационная основа обеспечения информационной безопасности приведена в п. 33 Доктрины информационной безопасности. Так, организационную основу системы обеспечения информационной безопасности составляют:

- Совет Федерации Федерального Собрания РФ;
- Государственная Дума Федерального Собрания РФ;
- Правительство РФ;
- Совет Безопасности РФ;
- федеральные органы исполнительной власти;
- Центральный банк РФ;
- Военно-промышленная комиссия РФ [81];
- межведомственные органы, создаваемые Президентом РФ и Правительством РФ;
- органы исполнительной власти субъектов Российской Федерации;
- органы местного самоуправления;
- органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Ключевым элементом, представленной системы является Президент РФ, определяет состав системы обеспечения информационной безопасности.

Одним из важнейших элементов структуры является ФСБ России, на которую согласно ст. 11.2 Федерального закона «О федеральной службе безопасности» [85], на службу возложены полномочия по формированию и

реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств.

ФСТЭК России [84] играет важную роль в осуществлении технического регулирования в области информационной безопасности. В частности, именно приказами ФСТЭК осуществляется определение требований к информационным системам, применяющимся в государственных органах и подведомственных им государственных предприятиях, а также контроль над выполнением указанных требований в ходе различных аттестаций и сертификаций.

В целом, можно назвать следующие государственные органы, которые осуществляет деятельность в сфере обеспечения информационной безопасности:

- Министерство Внутренних Дел РФ [72];
- Федеральная служба охраны России [78];
- Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) [44];
- ФТС России [82];

В последние десятилетия мы являемся свидетелями глобальной правительственной реформы – информатизации всех управленческих процессов [16, с. 3].

Однако следует отметить, что внедрение и функционирование цифровых технологий в государственном управлении зависит во многом от (политического) контекста, на который накладывается эта технология.

В настоящее время по данным ООН электронное правительство внедрено в 193 странах мира, элементами электронного правительства являются четыре типа взаимодействия:

- между органами госвласти;
- между органами госвласти и бизнесом;
- между органами госвласти и населением;

– между органами госвласти и госслужащими.

Информационные технологии создают определенные возможности для повышения эффективности развития демократического общества, с реализацией прав гражданского общества, развития внутренней реальной экономики, государственной политики и прочих процессов, направленных на активизацию всех сфер жизнедеятельности в современном мире.

Преимуществами внедрения информационных технологий в сферу публичного управления можно назвать следующие:

– предоставление государственных услуг на базе информационных технологий устраняет границу между государственными органами и гражданским обществом, обеспечивая каждому гражданину вне зависимости от его физических возможностей активно взаимодействовать с государственными служащими и различными ведомствами;
– использование информационных технологий в сфере публичного управления значительно сокращает время на взаимодействие между потребителями государственных услуг и государственными служащими, а также позволяет существенно экономить бюджетные средства;
– развитие информационных технологий в сфере публичного управления поднимает на новый уровень все оказываемые услуги, а также повышает качество межрегионального и межгосударственного сотрудничества;
– внедрение новых информационных средств (биометрические документы, средства идентификации, системы электронного архивирования) позволяют обеспечить доступ гражданам в любой точке планеты к необходимым им услугам, а также обеспечить их информационную безопасность;
– возможность вовлечения граждан посредством информационных технологий в управление территориями является принципом

развития гражданского и демократического общества, снижает социальную разобщенность, повышает сознательность и ответственность каждого гражданина [23, с. 14].

Таким образом, в основе организации управленческих процессов лежит информация, качество которой, а также характеристики движения определяют уровень и качество организации управления той или иной системой.

Применение в сфере управления цифровых технологий качественно изменяет организацию и эффективность управления. Цифровизация всех сфер общества, начиная от коммерческих и заканчивая социальными и публичными, обеспечивает различные векторы развития общественных отношений, наполняя их новым содержанием и возможностями. Модернизация общественных связей на основе информационных технологий ускоряет взаимодействие, обеспечивает безопасность участников таких отношений.

Федеральный принцип построения и реализации государственной власти является основой для формирования региональных органов власти и выполнения ими определенного объема полномочий. Так, конституционной региональные органы государственной власти наделены как собственными, так и делегированными полномочиями.

Процесс цифровизации деятельности органов исполнительной власти в г. Москве регулируется распоряжением Правительств г. Москвы № 1050-РП от 15.06.2005 «Об утверждении Концепции информатизации работы органов исполнительной власти, городских организаций в режиме «одного окна». Концепция регламентирует основные вопросы информационного обеспечения управленческого процесса, в частности, определяет участников цифровизации, определяет схемы подготовки и выдачи документов из Единого реестра, порядок работы «одного окна», порядок синхронизации и приведения стандартов обслуживания к единообразию.

Цифровизацию деятельности региональных органов исполнительной власти обеспечивает Программа «Электронная Москва». Основным

разработчиком программы является «Институт развития информационного общества». В первые годы реализации программы ее бюджет составлял до 5 193 114,00 т.р. При этом ежегодно среднее количество по цифровизации составляло 163. Самым дорогостоящим мероприятием стало «Создание системы обеспечения безопасности населения города (СОБГ)».

Информационное обеспечение департаментов составляет внутренний и внешний контур. Внутренний контур представляет собой обмен информацией внутри каждого Департамента (между руководителем и подчиненными, между сотрудниками), а внешний контур составляет обмен информацией между департаментами сферы управления городским хозяйством, обмен информацией с органами власти г. Москвы из других сфер, органами власти федерального значения, муниципальными органами власти, частными организациями и гражданами. Внешний контур частично может пересекаться с внутренним, если информация должна пройти обработку в Департаменте и запрашивающий должен получить ответ, либо она проходит вне его и направляется далее также по внешнему контуру.

Например, Департамент ЖКХ должен обмениваться информацией с Городскими центрами жилищных субсидий. Для обеспечения с одной стороны, субсидирования граждан при оплате услуг ЖКХ, а с другой, для компенсации организациям соответствующих затрат.

Обеспечение информацией соответствует основным направлениям деятельности Государственных казенных учреждений г. Москвы «Городской центр жилищных субсидий» (ГКУ «ГЦЖС»).

В первую очередь обеспечение информацией необходимо для развития отдельных сфер экономики города, в частности для реализации мер субсидирования жилищного строительства на территории г. Москвы. В настоящее время в жилищном секторе города сформировано множество проблем, тормозящих эффективное развитие территории и обеспечение повышения качества жизни населения.

Второе направление связано непосредственно с предоставлением льгот в сфере ЖКХ отдельным социальным группам населения. Уже сегодня реализуется ряд мер, направленных на предоставление компенсаций при оплате услуг ЖКХ 60 категориям граждан.

Третье направление связано с предоставление субсидий организациям сферы ЖКХ и компенсаций затрат, связанных с возмещением недополученных доходов, в результате реализации госпрограмм по предоставлению льгот гражданам Москвы при оплате коммунальных услуг. Например, Департамент имеет договорные отношения с управляющей компанией «ГЦЖС», по возмещению затрат организации, в результате недополученной прибыли.

Четвертое направление – возмещение управляющим организациям недополученных доходов в связи с применением государственных регулируемых цен.

Как можно заметить, в информационное обеспечение включается еще один тип организаций. Дополнительным участником внешнего информационного контура и одновременно поставщиком и получателем информации становятся управляющие компании. Данный участник взаимодействует с ресурсоснабжающими организациями, гражданами, организациями и предоставляет необходимую информацию органам исполнительной власти в сфере своей компетенции и полномочий. Кроме того, он взаимодействует с исполнительными органами в рамках контроля своей деятельности.

Пятое направление (с 2022 г.) – информационное обеспечение реализации прав отдельных льготных категорий граждан (ветеранов боевых действий и ветеранов военной службы) при оплате за жилищно-коммунальные услуги. Для реализации данного направления функционирует система приема, анализа и контроля обращений граждан по вопросам оформления жилищных субсидий.

Многочисленные потоки информации между участниками сферы управления городским хозяйством не всегда бывают защищенными, кроме того, в процессе информационного обеспечения могут возникать сбои и потери информации, что ведет к принятию неверных решений или простою.

Таким образом, организация применения информационных технологий в сфере управления в настоящее время требует тщательного анализа и оценки с точки зрения соответствия ее функционирования принципам безопасности и прозрачности. В ситуации, когда сфера информатизации и цифрового обеспечения деятельности региональных органов исполнительной власти монополизирована, а услуги государственным органам предоставляет одна единственная частная компания, возникают сомнения относительно информационной безопасности и отсутствия коррупционной составляющей.

Необходимо создавать организационно-правовые условия для возможности разработки платформы для реализации электронного правительства и применения широкого спектра информационных технологий в сфере регионального управления силами самого субъекта РФ либо предоставления ему на выбор услуг нескольких поставщиков. Приоритетным нам видится вариант разработки программы на федеральном уровне с последующей возможностью его доработки с учетом специфики каждого региона. Таким образом, на уровне государства будет разработано программное обеспечение для осуществления федерального, регионального и муниципального управления, которое впоследствии будет дорабатываться и обновляться в соответствии с потребностями каждого пользователя (субъекта РФ, министерства, департамента).

Единообразный подход к применению информационных технологий в региональном управлении на государственной платформе обеспечит унификацию информационного процесса, возможность привлечения лучших специалистов, экономию бюджетных средств, большую прозрачность и исключение коррупционного фактора.

Также с необходимо оценить перспективы использования открытого кода для разработки программного обеспечения электронного правительства. Открытый код должен предоставить возможность постоянного его совершенствования специалистами, выявления и устранения системных ошибок, повышения эффективности и безопасности системы в целом. В любом случае, данный вопрос должен быть тщательно разработан теоретиками и практиками с учетом опыта зарубежных государственных органов и частных компаний.

По итогам 2021 года в рамках Программы в промышленную эксплуатацию были введены 11 Государственных информационных систем и 4 Информационные системы [42].

Основным документом информатизации и информационного обеспечения деятельности региональных органов власти является Распоряжение Правительства РФ «Об утверждении Концепции региональной информатизации» [58].

Концепция регламентирует следующие вопросы:

- использование информационно-коммуникационных технологий для социально-экономического развития регионов (применение информационных технологий в публичной управленческой сфере);
- повышение качества предоставления государственных и муниципальных услуг (обеспечение открытости деятельности органов региональной власти);
- обеспечение доступа граждан к информации о деятельности органов государственной власти субъектов РФ и органов местного самоуправления (материальный и образовательный аспект информатизации регионов);
- организационное и инфраструктурное обеспечение региональной информатизации.

Для реализации Концепции на уровне Правительства РФ, в частности, Министерства цифрового развития, связи и массовых коммуникаций РФ

обеспечивается методическая помощь. Для этих целей был сформирован Совет по региональной информатизации.

Одним из направлений цифровизации является обеспечение цифровой безопасности. Обеспечение информационной безопасности на всех уровнях государственного управления, а также в сфере общественно-экономических отношений осуществляется на основе Доктрины информационной безопасности. Доктрина оперирует понятием «информационная инфраструктура», которая включает в себя объекты информатизации и информационные системы. Именно эти информационные объекты являются первоочередной целью обеспечения безопасности согласно Доктрине, при этом объекты, основанные на цифровых технологиях, которые в связи с развитием технологий на определенном этапе могут выйти за рамки понятия объектов информатизации и информационных систем, оказываются вне сферы регулирования Доктрины, т.е. определенный сегмент цифровой экономики и государственного управления может выпадать из сферы обеспечения безопасности.

В условиях технологической изоляции и необходимости самообеспечения развития информационных и цифровых технологий руководством страны был принят ряд нормативных актов, обеспечивающих регулирование применения и оборота информационных технологий. К таким актам следует, прежде всего, отнести Стратегию развития информационного общества на 2017-2030 годы, утверждённую Указом Президента Российской Федерации от 9 мая 2017 г. № 203 [79], а также Национальную программу «Цифровая экономика Российской Федерации» [39], которая пришла на смену Программе «Цифровая экономика РФ».

Попытаемся выявить способы обеспечения безопасности применения цифровых технологий в сфере регионального управления на основании данных актов.

Стратегия развития информационного общества на 2017-2030 годы направлена на создание условий для формирования свободы доступа к

информации, свободы выбора источников информации, сохранение традиционных способов получения информации. Стратегия оперирует понятиями и категориями информационных и коммуникационных технологий (общество знаний, информационная структура, Национальная электронная библиотека), при этом в Стратегии упоминаются инструменты цифровых технологий (облачные хранилища, туманные вычисления, Интернет вещей и т.д.), в Стратегии также говорится о предоставлении государственных и муниципальных услуг, которые осуществляются посредством цифровых технологий, при этом само определение цифровых технологий в тексте документа отсутствует.

Обеспечение безопасности в государственном управлении в Стратегии связывается с применением «безопасного программного обеспечения», созданного по отечественным разработкам и с применением отечественных составляющих. Критерии безопасности программного обеспечения устанавливаются и проверяются уполномоченным органом государственной власти. Также в Стратегии ставится задача постепенной замены импортного программного обеспечения и зарубежных комплектующих и формирование информационного и цифрового пространства, независимого от иностранных технологий.

Акцент на развитии и обеспечении безопасности цифровых технологий мы находим в Программе «Цифровая экономика Российской Федерации». Программа включает несколько направлений развития, в том числе: «Нормативное регулирование цифровой среды», «Кадры для цифровой экономики», «Информационная инфраструктура», «Информационная безопасность», «Цифровые технологии», «Цифровое государственное управление». Особый интерес для нас представляют последние направления, в которых напрямую обозначена цель развития цифровых технологий и обеспечения в данной сфере безопасности.

Направление Программы «Кадры для цифровой экономики» создает условия для повышения грамотности населения в сфере информатизации и

цифровизации, развитие необходимых компетенций для обслуживания цифровой экономики, переквалификации служащих для работы в технологически новых условиях.

С точки зрения необходимости самостоятельного развития цифровых технологий следует обратить внимание на направление Программы «Цифровые технологии», в котором цифровые технологии выделяются в качестве самостоятельного предмета развития и регулирования в рамках информатизации общества. Данное направление ставит целью коммерциализацию отечественных наработок, поддержку и внедрение цифровых технологий в экономику и популяризацию цифровых технологий посредством цифровизации деятельности крупнейших российских компаний.

Информационные технологии могут непосредственно влиять на структуры данных государственного управления, усиливая или ослабляя традиционные иерархические формы.

В настоящее время в РФ обеспечение цифровизации государственного управления осуществляется в рамках направления «Цифровое государственное управление». Задача направления – расширить перечень и повысить эффективность предоставляемых услуг посредством цифровизации взаимодействия граждан и государственных и муниципальных органов. Безопасность взаимодействия граждан и государственных и муниципальных органов обеспечивается на основании применения отечественных цифровых разработок, а также применения программного обеспечения, созданного в рамках импортозамещения.

На поддержание безопасности применения цифровых технологий в сфере государственного управления направлено снижение объемов используемого программного обеспечения – менее 10% от закупаемого или арендуемого для государственных и муниципальных нужд. Также для этой цели планируется перевести маршрутизацию российского сегмента сети Интернет на российскую территорию, повышение защищенности

используемого программного обеспечения и использование средств цифровой защиты.

Для оценки цифровизации регионального управления в Правительстве РФ были разработаны критерии, на основании которых субъектам РФ присваивались баллы для выстраивания рейтинга информационного обеспечения деятельности региональных органов государственной власти. Критериями эффективности электронного правительства в настоящее время являются:

- качество внедрения информационных технологий и платформ, обеспечивающих обратную связь;
- наличие мер государственной поддержки ИТ-отраслей, например, установление льгот, снижение налоговой нагрузки, предоставление грантов, компенсаций и пр.;
- обеспечение информационной безопасности, например качество контроля за сохранностью конфиденциальных данных;
- развитие мер импортозамещения при внедрении платформ ИТ отечественного производства в систему государственного управления и др.

В каждом регионе в настоящее время приняты региональные стратегии цифровизации, что обеспечивает продвижение по рейтингу Правительства о цифровой зрелости регионов.

В настоящее время в Республике Татарстан активно реализуются программы цифрового развития территории, охватывающие более 15 отраслей экономики региона. В различные отрасли экономики внедряются современный информационные и цифровые платформы, платформы искусственного интеллекта, Биг-дата и пр.

Уже к 2024 году в Республике Татарстан уровень доступности государственных услуг в электронном виде должен составить 95%. В Москве и Московской области, а также в северной столице РФ данный показатель варьируется в пределах 95-97% к концу 2024 года [66].

В транспортной отрасли прогнозируется развитие и внедрение цифровых технологий, направленных на создание эффективной цифровой модели дорожной сети, которая была бы адаптирована к системе управления дорожным движением.

В городе Москва в системе государственного управления огромную роль играет формирование модели цифрового помощника для населения и обеспечения реализации мер, направленных на поддержку малого и среднего бизнеса. В сфере промышленности огромную роль играют меры, направленные на создание цифровых технологий, внедряемых в промышленные предприятия и организации с целью повышения промышленных мощностей и обеспечения выпуска наиболее конкурентоспособной продукции на рынок.

В отрасли сельского хозяйства цифровая трансформация также играет огромную роль, особенно в системе управления за отдельными сельскохозяйственными объектами, например в настоящее время активно внедряется система оповещения для пчеловодов, а также система идентификации крупного рогатого скота.

В Республике Татарстан активно внедряются информационные технологии в сферу культуры, например в настоящее время реализуется проекты, связанные с развитие музейной информационной системы, а также с внедрением цифрового пространства в различные мероприятия, связанные со сферой культуры и туризма, что оказывает огромное воздействие на социально-экономическое развитие территории и привлечение туристов в регион.

В Санкт-Петербурге в настоящее время реализуется стратегия цифровой трансформации, которая включает в себя 11 отраслей экономики. В первую очередь информационное пространство развивается на основе внедрения информационных технологий в медицинские учреждения, такие как нейротехнологии и искусственный интеллект. В промышленных предприятиях активно используется робототехника и сенсорные компоненты,

в системе государственного управления используется система большие данные и пр.

В системе медицинского здравоохранения информационные технологии все больше приобретают важное значение, поскольку играют решающую роль в повышении качества жизни населения. В северной столице РФ в проекте стратегии развития цифрового пространства к 2024 году более 10% медицинских организаций государственной и муниципальной системы здравоохранения должны использовать информационные медицинские решения, направленные на повышение качества диагностики и лечения пациентов.

Не менее важной задачей стратегии цифрового развития Санкт-Петербурга является развитие городской среды и жилищно-коммунальной сферы. Сегодня обеспечивается внедрение цифровых сервисов в жилищно-коммунальную сферу, а также в развитие беспилотного транспорта в рамках развития городской среды. В транспортной отрасли наблюдается активное внедрение систем видеонаблюдения в режиме реального времени и пр.

Санкт-Петербург является одним из городов федерального значения, в развитии которого важную роль играет сфера туризма. В сфере туризма предусмотрены меры использования зарубежного опыта при внедрении информационных программ, так, например планируется оцифровка деятельности поставщиков продуктов туристического продукта и создание специального портала, на котором будет размещена вся информация о гидах и экскурсиях города.

В настоящее время в Санкт-Петербурге планируется внедрение информационных технологий в сферу физической культуры и спорта, например внедрение единой платформы реестра лиц, которые занимаются спортом.

В настоящее время в Московской области реализуется несколько проектов цифрового развития, которые включают в себя более десяти

отраслей: транспорт и связь, медицина, образование, культура, государственное управление и др.

В ходе реализации стратегии цифрового пространства внедряются такие информационные системы: как искусственный интеллект, промышленный интернет, биометрические технологии, блокчейн. Огромное значение в Стратегии развития цифрового пространства Московской области приобретает сфера образования, так результатом задачи цифрового пространства сферы образования к 2024 году должен стать переход 90% студентов на цифровой профиль и создание цифрового помощника учителя, за счёт которого будет повышено качество дистанционного образования и полностью автоматизирована система верификации.

В рамках развития сферы здравоохранения к 2024 году 100% граждан должны иметь электронное медицинские карты, позволяющие обеспечить необходимый уровень доступности государственной услуг и повысить качество медицинского обслуживания. Кроме того, к 2024 году планируется достигнуть уровня 30% перевода всех консультаций с использованием видеоконференций в взаимодействии врача и пациента.

В здравоохранении Московской области планируется, что уже к 2024 году 70% назначений врачей будут осуществляться гражданами дистанционно.

В Калмыкии в рамках развития отрасли транспорта планируется к 2024 году оснастить более 40% автобусов безналичной системой оплаты за проезд, аналогичный показатель установлен и в Республике Татарстан, в настоящее время данный показатель составляет 76%, в Московской области данный показатель составляет 100%.

Однако, есть ряд проектов, которые значительно опережают богатые субъекты РФ, например в Калмыкии установлен показатель к 2024 года перехода 81% граждан на электронные медицинские карты, в Санкт-Петербурге данный показатель установлен лишь на уровне 19%.

В Алтайском крае стратегия развития информационных технологий и цифрового пространства охватывает более 11 отраслей экономики: транспорт и связь, образование, туризм, здравоохранение, промышленность и пр. Активно внедряются такие информационные системы как: искусственный интеллект, нейротехнологии, интернет вещей, блокчейн, робототехника и др. Некоторые проекты включает в себя показатели, которые указаны неясным образом. Основной задачей развития информационных систем в отрасли сельского хозяйства является внедрением системы моя цифровая ферма, однако в качестве основного показателя выступает показатель достижения цифровой зрелости. Таким образом, цифрового показателя как такового нет, а лишь представлена задача внедрения цифровых технологий в отрасль сельского хозяйства на основе проекта моя цифровая платформа.

Как и в Калмыкии, в Алтайском крае в 2024 году будет довольно низкая доля студентов, для которых ведется цифровой профиль, – 20%.

Рассматривая стратегии цифрового развития курганской области и Омской области, отметим следующее. Стратегия цифрового развития Курганской области охватывает более 15 отраслей экономики. К 2024 году уровень доступности государственных услуг социальной сферы должен достигнуть уровня 95%, что является достаточно высоким показателем среди субъектов РФ и приравнен к богатым регионам страны.

Запланирован широкий портфель проектов практически для всех выбранных отраслей. К 2024 году в сфере образования планируется достичь 50% охвата всех студентов цифровым профилем, а более 20% студентов будут подключены к системе федеральной информационно-сервисной платформы, позволяющей получить качественное образование в сфере дистанционного образования. Наряду с богатыми регионами также планируется внедрение суперсервиса «Поступление в университет онлайн».

Однако, до сих пор остается неясным показатель внедрения информационных технологий в сферу промышленности Курганской области. В то же время Курганская область - единственный из рассмотренных в статье

регионов, где отрасль «Торговля и предпринимательство» выделена в стратегии цифровой трансформации. Планируется внедрение электронной коммерции в сферу торговли, что поможет сократить уровень безработицы в регионе и увеличить объем розничного товарооборота.

В отрасли образование в Омской области важную роль приобретает создание высокопроизводительного вычислительного центра, к 2024 году планируется подключить к данной системе более 10 организаций, в частности научных организаций, в которых суперкомпьютерный центр будет ориентирован на выпуск конкурентоспособной продукция в сфере науки и разработок.

В настоящее время Омская область и Курганская область участвуют в федеральном проекте «беспилотники для пассажиров и грузов», однако, в стратегиях неясном остаётся момент с какими показателями взаимосвязан данный проект, неясном остаётся и доля транспортных услуг, которая предоставляется в электронном виде.

В жилищно-коммунальной сфере планируется в Омской области к 2024 году достичь 32% использования электронных платежей при оплате за коммунальными услугами.

Таким образом, в современных условиях развития цифровых технологий, внедрения их в национальную экономику и государственное управление, вопросы цифровизации и цифровой безопасности стоят крайне остро. Решение данной задачи силами отечественных разработчиков и производителей видится логичным и обоснованным. При этом организационно-правовое обеспечение и стратегическое регулирование развития и внедрения цифровых технологий в сферу государственного управления не отвечает потребностям данной сферы.

В связи с изложенным целесообразно выделить в законодательных и плановых документах понятие «цифровые технологии», как самостоятельный предмет регулирования, что обеспечит выделение развития цифровых технологий в самостоятельное направление, а также позволит создать

нормативную основу регулирования на ближайшие несколько лет, когда инструменты цифровых технологий будут в некоторой степени непредсказуемо изменять окружающую действительность.

## 2.2 Вопросы обеспечения информационной безопасности в деятельности органов государственной власти

В настоящее время органы региональной власти сталкивается с глобальной цифровизацией. Следовательно, необходимо изложить аргументы по определению места информационных технологий в государственном управлении и систему возможных проблем при их внедрении, а также перспективы развития информационных технологий в сфере государственного управления.

Процесс оцифровки предполагает свободный поток информации от государственных органов к представителям широкой общественности и третьим сторонам, таким как организации гражданского общества и средства массовой информации, а также от представителей широкой общественности и третьих сторон к государственным органам.

При этом в настоящее время в РФ наблюдается тенденция, когда информационно-коммуникационные технологии все больше развиваются в частном секторе, в то время как государственные органы, в частности на региональном и местном уровнях, используют бюрократическую форму управления.

Успешное преодоление проблем информационного пространства в региональном государственном управлении не может быть предусмотрено без успешного совершенствования законодательства об использовании информационных технологий в государственном управлении в связи с внедрением новых информационных технологий и систем.

В системе государственного управления на региональном уровне по обеспечению информатизации и внедрения систем электронного

правительства возникает ряд проблем, связанных с нарушением использования электронной цифровой подписи.

Актуальными вопросами сегодня являются совершенствование законодательной базы в области регулирования использования электронной подписи на государственном уровне, с учётом минимизации рисков мошенничества и создания единой системы информационной безопасности.

Кроме того, актуальными вопросами являются оптимизация использования электронной подписи без присутствия нотариуса и возможности получения сертификата электронной подписи в электронном виде, посредством онлайн-сервисов.

В настоящее время невозможно эффективно развивать цифровую экономику и электронный документооборот без использования электронной подписи, однако, использование электронной подписи порождает увеличение количества мошеннических схем, в результате чего снижается эффективность системы государственного управления на региональном уровне, а также возникают проблемы, связанные с утечкой персональных данных.

В системе использования электронной подписи актуальной проблемой до сих пор остаётся проблема недостаточного регулирования процессами идентификации, прежде всего с целью совершенствования использования системы электронной подписи необходимо использовать модель надзора за выпуском сертификатов со стороны органов налоговой службы, например за счёт приостановления либо отзыва сертификация при возникновении случаев мошенничества. Следующей мерой должно стать создание единой платформы, выпущенных сертификатов в объединенный реестр, который позволяет уведомлять пользователей о том, что электронная подпись была получена в конкретном удостоверяющем центре (УЦ).

Современные информационно-коммуникационная технологии дают новые возможности в развитии и совершенствовании системы государственного управления, поэтому решение текущих проблем внедрения

информационных технологий на государственном уровне играет значимую роль.

Во многом успех трансформации государственного управления в эпоху цифровизации напрямую связан с усилиями и ресурсами, выделяемыми органами государственного сектора на реализацию стратегий.

В РФ объем инвестиции на развитие информационных технологий и их внедрение в различные сферы экономики ежегодно увеличиваются, при этом данная тенденция будет сохранена на протяжении нескольких лет. Тем не менее, процесс выделения бюджетных ресурсов на развитие цифровых платформ имеет спонтанный характер, особенно на региональном уровне, поскольку объём выделяемых средств иногда недостаточен, что приводит к сдерживанию цифрового развития. В настоящее время наибольшая доля затрат — это затраты на компьютерзацию, а также затраты на обучение государственных служащих. Уровень компетенции государственных служащих на всех уровнях государственного управления является объединяющим элементом, порождающим фактором в реализации как макроинституциональных, микроинституциональных, так и технических условий для трансформации государственного управления в эпоху цифровизации. Поэтому, в каждом регионе должно уделяться особое внимание обучению специалистов при внедрении информационных технологий, позволяющих обеспечить качество системы государственного управления.

Важными мерами развития информационных технологий в системе региональной исполнительной власти являются:

- институциональная поддержка и ее развитие;
- создание аналитических порталов с целью обеспечения общественного контроля;
- повышение уровня подотчетности, прозрачности, активности государственных служащих;
- реализация проектов электронного правительства.

Необходима качественная разработка системы электронных коммуникаций государственного управления в каждой конкретной государственной структуре на межведомственном уровне [10, с. 15].

Кроме того, необходимо внедрить продуктивный онлайн-диалог между всеми заинтересованными сторонами, направленный на повышение конкурентоспособности государственных служащих и поддерживать систему постоянного детального контроля за процессы в соответствующей области в режиме реального времени на веб-сайте департаментов.

Решение выявленных проблем позволит значительно повысить эффективность цифровизации в сфере государственного управления на региональном уровне, поскольку использование информационных технологий в государственном управлении значительно экономит время, затрачиваемое на решение различных задач то способствует динамике государственного развития и прозрачности менеджеров.

Важным направлением дальнейших практических изысканий государственных менеджеров, юристов, программистов будет попытка составить список системы эффективных онлайн-платформ для ведения дел электронного правительства.

Цифровая модель управления регионом должна быть создана на цифровой платформе, благодаря которой будет анализироваться вся информация о данном регионе.

Благодаря данному инструменту системы управления территорией можно эффективно проводить мониторинг и регулировать планируемые показатели развития территории.

В начале 2000-х годов отсталость России в области цифровых технологий была очевидна для нового российского руководства, поскольку государственный сектор практически не демонстрировал признаков прогресса в этой сфере. В то время как мировые лидеры постепенно переходили к новой программе цифровизации, России оставалось только провести полноценную реформу государственного сектора.

В результате реализации программы «Информационное общество» целью является создание новой телекоммуникационной инфраструктуры в России, которая позволит значительно снизить коммерческие и финансовые затраты за счет стандартизации среды взаимодействия, процессов и достижения технической независимости России в использовании информационных технологий.

В настоящее время уровень внедрения компьютерного оборудования, отвечающего современным требованиям, в системе государственного управления в РФ находится на достаточном уровне (но с учетом наложенных западными странами санкций и сложностей с поставками нового современного оборудования).

Среди информационных технологий, которые являются наиболее распространенными в системе государственного управления, стоит отметить стандартные инструменты, которые активно используются на всех уровнях государственной власти.

В регионах для реализации цифровых технологий в региональном управлении создаются департаменты информационных технологий. Работа департаментов направлена на взаимодействие с жителями города, представителями бизнеса и создание общей инфраструктуры.

Постепенно расширяется информатизация и автоматизация отраслей городского хозяйства, так, были внедрены информационные системы Единая медицинская информационно-аналитическая система, единая образовательная платформа, объединяющая педагогов, учеников и родителей.

На региональном уровне, в ходе проведенного исследования информационного обеспечения деятельности органов государственной власти отмечено, что в настоящее время активно организуется работа по внедрению электронного правительства в субъектах РФ, а также в муниципалитетах, для достижения целей развития информационного общества и информационного пространства используется программно-ориентированной подход, который позволяет решить комплекс основных задач, связанных с внедрением систем

электронного правительства на региональном уровне, а именно решение задач по повышению качества жизни населения и достижения экономического роста на региональном уровне.

Благодаря дальнейшему совершенствованию и внедрению информационных технологий в систему государственного управления на региональном уровне будет усилен общественный контроль за использованием бюджетных ресурсов, рациональным распределением их в различные сферы экономики, что соответственно приведёт к повышению экономической устойчивости и социально-экономического развития различных регионов страны, а также приведет к повышению эффективности взаимодействия органов региональной и муниципальной власти с обществом и экономикой в целом по решению различных социальных и экономических задач.

Анализ организации информационного обеспечения на региональном уровне позволил выявить, что созданы и успешно функционируют системы, обеспечивающие сбор, обработку и обмен информацией между региональными органами власти. Одновременно с этим существует разрыв между информацией, циркулирующей в сфере государственного управления и информацией, которая потребляется и производится жителями города, и представителями бизнеса. В связи с этим возникает задача разработать и внедрить системные связи между частным и публичным сектором, что обеспечит сбор информации, необходимой для разработки планов развития города, анализа эффективности реализованных и планируемых мероприятий, оценки степени внедрения тех или иных решений.

Общее направление развития цифрового обеспечения должно включать следующее:

– постепенную интеграцию информационного пространства публичной и частной сферы;

– разработка инструментов и технологий для разграничения объема полномочий пользователей и обеспечения мониторинга их активности;
– преобладание в сфере управления программ с открытым кодом, что обеспечит постоянное выявление недостатков и их устранение и совершенствование цифровых инструментов.

Также представляется важным транслирование опыта в другие регионы, что обеспечит постепенное слияние региональных информационных систем. Благодаря этому будет облегчен сбор массива данных, их аналитическая обработка и принятие на их основе решений регионального и федерального уровня.

Решение представленных проблем, может быть обеспечено за счет реализации следующих ряда условий [29, с. 210].

Средства визуализации должны позволять провести детализацию событий непосредственно на картографическом фоне или во временной ретроспективе, кроме того, необходимо визуализировать степень участия, полномочия и уровень ответственности участников данных процессов. Для большей наглядности представленные схемы должны быть «живыми», т.е. отображать текущие данные в точках измерения и/или позволять вызвать график значений различных параметров за заданный период. Средства визуализации должны позволять сравнивать графики путем наложения с элементами прозрачности, а также проводить другие манипуляции с информационными ресурсами, соответствующие режиму визуализации пространственных данных.

Сбор информации должен происходить автоматически в течение всего бюджетного периода, это процесс должен решаться оперативно без пересылки документов между организациями. Современные технологии позволяют включать в управленческие процессы сторонние организации, партнеров, клиентов и пр. для формирования единого потока работ. Необходимо предоставить возможность информировать подведомственные организации,

ведомства, получателей услуг об этапе реализации того или иного проекта с учетом политики информационной безопасности, формировать информационный контент под конкретного потребителя информации, упрощая документооборот и сокращая время операций.

Очистка и верификация данных, поступающих от телеметрии, должна обеспечить высокое качество учета и технологического обеспечения процессов контроля управленческой системы и состояния реализации задач.

Создание событийной архитектуры необходимо для обеспечения эффективного мониторинга параметров и критериев управленческих процессов: планирование бюджетных доходов и расходов, проектное планирование деятельности на бюджетный период, отчет по реализуемым проектам.

Архитектура системы должна позволять оперативно реагировать на критические показатели, например, в рамках организации закупок для государственных и муниципальных нужд, проводить мониторинг действия служащих, т.е. фиксировать ответственность каждой управляющей единицы, анализировать результативность и эффективность корректирующих действий, формировать пакет рекомендаций по определенным типам событий.

Перспективные развития информационного обеспечения деятельности органов государственной власти должны учитывать следующие факторы:

Во-первых, развитие целесообразно только после перехода на облачную платформу, т.к. реализация, внедрение и поддержка новой функциональности в текущей архитектуре существенно более затратно, чем модернизация ЕИТП и дальнейшее его развитие в совокупности

В основу развития должны быть положены принципы:

- работа с большими данными и соответствующие компоненты новой платформы;
- внедрение элементов искусственного интеллекта;
- передача управления в части настройки и модификации бизнес-процессов на уровень пользователей;

– мониторинг, поиск зависимостей и отклонений в реальном масштабе времени по всей системе и всему региону.

Во-вторых, развитие функциональности осуществляется:

– в процессе сопровождения в части небольших доработок;
– в рамках отдельного проекта, формируемого на основе концепции развития.

Таким образом, предлагаемая система направлена на объединение на своей базе всех сервисов, структур и подсистем, посредством которых осуществляется управление на региональном уровне. Возможность интеграции системы с другими системами позволяет реализовывать совместные проекты на уровне государства, общественности и частного бизнеса.

Для реализации проекта необходимо: разработка и адаптация программного обеспечения; интеграция существующих систем; наладка систем взаимодействия со сторонними программами и сервисами; размещение средств визуализации; обучение сотрудников.

Унифицированный характер предлагаемого проекта позволит с учетом незначительной адаптации под специфику других регионов, внедрить его в любой территориально-административной единице.

Создание глобальной информационной системы повысит эффективность управления на большей территории, поскольку оперирование большими массивами данных, учет эффективного опыта различных регионов позволит более точно и эффективно планировать будущую деятельность.

Функциональность предлагаемой системы позволит в значительной степени сократить количество государственных и муниципальных служащих, выполняющих в настоящее время действия по сбору и обработке информации. Предполагается, что количество служащих можно будет сократить на 10-15 %.

В результате внедрения системы будет создана область:

– участия граждан в планировании расходов бюджетных средств путем подачи собственных предложений и проектов;

– взаимодействия государственных и муниципальных структур на цифровой платформе;
– облачного массива данных для обеспечения анализа, мониторинга, оценки и планирования управленческих действий на уровне региона.

Внедрение системы позволит выполнять следующие действия:

– построение карт закупок для государственных и муниципальных нужд. Анализ движения бюджетных средств, отслеживание заключенных договоров между государственными органами и представителями бизнеса. Выявление коррупционных схем;
– составление массива данных о движении бюджетных на основании различных способов классификации: средств по отраслям, по субъектам-получателям бюджетных средств и т.д.;
– отражение эффективности деятельности департаментов, управлений и ведомств;
– возможность составления проектной деятельности в рамках совместных проектов с участием государственных органов и представителей частного бизнеса;
– отслеживание расходования бюджетных средств в соответствии с планами деятельности каждого ведомства;
– оценка эффективности деятельности согласно заранее установленным критериям;
– проведение аналитики по таким аспектам как: участие граждан в управлении, удовлетворение запросов граждан, уровень взаимодействия государственных и муниципальных органов с гражданами, представителями общественности и бизнесом [98].

Подключение дополнительного функционала, интеграция с иными платформами дадут возможность расширять сферу взаимодействия и увеличат функциональные возможности системы.

Выводы по второй главе выпускной квалификационной работы.

Во-первых, целесообразно выделить в законодательных и плановых документах понятие «цифровые технологии», как самостоятельный предмет регулирования, что обеспечит выделение развития цифровых технологий в самостоятельное направление, а также позволит создать нормативную основу регулирования на ближайшие несколько лет, когда инструменты цифровых технологий будут в некоторой степени непредсказуемо изменять окружающую действительность.

Во-вторых, общее направление развития цифрового обеспечения должно включать следующее: постепенную интеграцию информационного пространства публичной и частной сферы; разработка инструментов и технологий для разграничения объема полномочий пользователей и обеспечения мониторинга их активности; преобладание в сфере управления программ с открытым кодом, что обеспечит постоянное выявление недостатков и их устранение и совершенствование цифровых инструментов. Также представляется важным транслирование опыта в другие регионы, что обеспечит постепенное слияние региональных информационных систем. Благодаря этому будет облегчен сбор массива данных, их аналитическая обработка и принятие на их основе решений регионального и федерального уровня.

# Глава 3 Проблемы обеспечения информационной безопасности в сфере образования и воспитания

## 3.1 Организационно-правовые основы обеспечения информационной безопасности в сфере образования и воспитания

В связи с утверждением Президентом РФ в 2022 году Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» [80] важное значение приобретает проблема информационной безопасности в сфере образования и воспитания детей.

Проблема обеспечения информационной безопасности подрастающего поколения в процессе воспитания и образования имеет междисциплинарный характер. Поэтому внимание ей, помимо представителей юридической науки, уделялось психологами, педагогами, философами, политологами.

Надо сказать, что в последнее время эта проблема серьезно озаботила научное сообщество, что лишний раз подтверждает ее актуальность.

Так, М.С. Журавлев, критически оценивая современное законодательство в части обеспечения безопасности в информационной сфере, пишет: «Однако действующее законодательство в сфере информационной защиты личной информации далеко не конструктивно и зачастую расходится с этическими принципами, которые позволяют корректно оценить моральные и нравственные масштабы нанесенного человеку вреда при разглашении его личной информации» [19, с. 43].

Значительная работа по изучению угроз в информационно-психологической сфере проведена К.Д. Рыдченко [62, с. 349]. Он, в частности подвергает критике положения Доктрины информационной безопасности за ее приверженность «интересам сохранения» в ущерб «интересам развития»: «Анализ перечисленных в данном акте интересов позволяет сделать вывод о тотальном преобладании «интересов сохранения» над «интересами развития»,

то есть Доктрина информационной безопасности не создает перспективу развития системы обеспечения информационно-психологической безопасности» [62, с. 349]. Кроме этого, К.Д. Рыдченко обращает внимание на чрезмерно широкую трактовку органами государственной власти свободы слова, печати и массовой информации, не приемлющую исключений из этого правила и провоцирующую оборот вредоносной информации [62, с. 350]. При этом автор не выделяет особо проблему воздействия деструктивной информации на подрастающее поколение.

М.Ф. Алиева не без основания утверждает, что «от обеспечения информационной безопасности существенно зависит национальная безопасность России, и эта зависимость будет значительно возрастать в ходе технического прогресса и проникновения информационных технологий во все сферы деятельности современного общества» [4, с. 98]. Автор предлагает комплексный метод решения проблем информационной безопасности. В частности, по ее мнению, «органы государственной власти должны создать непротиворечивую нормативную базу, учитывающую все аспекты проблемы информационной безопасности» [4, с. 98].

О необходимости создания четкого юридического оформления при разработке нормативных актов, регулирующих деятельность органов информационной безопасности, говорит Э.М. Брандман [11, с. 68]. Он высказывается за создание института информационного патроната со стороны государства: «Информационная защита достигается путем внесения в порядке законодательной инициативы законопроектов, подпадающих под юрисдикцию органов информационной безопасности, осуществления судебной защиты, проведения оперативных мероприятий силами и средствами информационной безопасности» [11, с. 69].

М.А. Трухачева считает, что при незначительной зависимости индивида от доступности информации и распространенности современных технических средств связи нормативно-правовая база безопасности Всемирной сети

сегодня не апробирована ни временными рамками, ни общественными нормами [70, с. 83].

Н.Н. Пономарев обращает внимание на глобализацию, как фактор усиливающий несовпадение интересов государств, конкуренцию, направленную на усиление влияния на мировую политику, что создает прямую угрозу национальной безопасности нашей страны [43, с. 78].

Ф.В. Ахмадиев увязывает появление негативных тенденций в сфере информации с ее коммерческой составляющей: «Вторжение в информационное пространство товарно-денежных отношений привело к появлению в среде руководителей СМИ прослойки идеологов «новой» морали, которые делают заявления, что информация – это товар, а значит писать и вещать сегодня нужно только за деньги. Нет сомнения в том, что такая коммерциализация журналистики вредна для общества» [6, с. 34].

А.А. Марков призывает государство «выполнять управленческие функции, направленные на интернационализацию информационной деятельности российских средств массовой коммуникации, с обязательным учетом и даже приоритетом национальных интересов в этой сфере, а также противодействовать иностранной информационной экспансии, тем самым реально влияя на степень информационной защиты общества от глобальной информационной экспансии» [36, с. 312].

Таким образом, современная наука сформулировала ряд положений, которые не оставляют сомнения в наличии потенциального роста угроз государственным и общественным институтам в связи с процессами глобальной информатизации.

Среди информационных угроз особую опасность представляют те, которые оказывают влияние на подрастающее поколение. В частности, Л.А. Гаязова считает, что «из совокупности основных социальных проблем, характерных для российского общества, особую опасность представляют те, что затрагивают процессы формирования личности подрастающего поколения и оказывают непосредственное влияние на систему отношения детей,

подростков и молодежи к социальным явлениям, к другому человеку и к себе самому» [14, с. 65].

О.С Безугленко с беспокойством говорит о причинах нарастания угроз информационной безопасности несовершеннолетних. Они, по ее мнению, кроются «как в возрастающей зависимости человека и общества от информационной продукции, так и в реализации экономических и политических интересов с использованием новых информационных и телекоммуникационных технологий, в том числе при распространении информации негативного содержания» [9, с. 66]. Бесконтрольное использование информационных материалов негативного характера «нередко оказывает на детей психотравмирующее и растлевающее влияние, побуждает их к рискованному, агрессивному, жестокому, антиобщественному поведению, облегчает их вовлечение в криминальную деятельность, развратные действия, азартные игры, тоталитарные секты и иные деструктивные организации» [9, с. 67].

А.И. Савельева обращает внимание на то, что «несмотря на предпринимаемые усилия со стороны органов государственной власти по закрытию интернет-сайтов с опасным для психики несовершеннолетних контентом, в информационно-телекоммуникационной сети Интернет все еще можно найти общую информацию о подготовке и разновидностях самоубийства» [63, с. 62].

О необходимости обеспечения психологической безопасности образовательной среды пишет О.В. Люсова [35, с. 134]. С.Л. Яблочников и И.О. Яблочникова под угрозой психологической безопасности в системе образования понимают «совокупность реальных и гипотетических воздействий (внутренних и внешних) на ее активные элементы и систему в целом, которые прямо или косвенно могут нанести ущерб психологическому здоровью участников образовательных процессов» [97, с. 141].

А.В. Андреева рассматривает с точки обеспечения психологической безопасности такую дефиницию как «духовность» [5, с. 25]. А.Г. Колгатин

ставит целью своей работы описание комплексной системы угроз информационной безопасности личности и общества в системах открытого образования [31, с. 418].

В контексте изучаемой проблемы необходимо обратить внимание на установленную в научных исследованиях взаимосвязь между информационным воздействием на молодежь и проблемой информационных войн. В частности, А.Д. Желонкин анализируя методы искажения информации с политическими целями, отмечает: «С сегодняшним развитием информационных технологий информационная война стала наиболее опасна, поскольку осуществляется посредством сети Интернет. Методами информационной войны является распространение дезинформации или представление информации в выгодном для одной стороны свете, что в перспективе должно обеспечить переход на сторону ведущего информационное воздействие» [18, с. 153].

Многими авторами отмечается трудность правового регулирования в связи с ограничениями принципиального характера. Так, один из исследователей проблем обеспечения информационной безопасности К.Д. Рыдченко высказывает интересные замечания относительно дефиниции понятия «цензура». Являясь сторонником точки зрения, согласно которой «киберпространство… действительно требует нормативного вмешательства государства» [60, с. 40], он предлагает не отождествлять политическую цензуру, которая прямо запрещена Конституцией РФ (ст. 29) с наложением запрета на распространение информации, наносящей вред пользователям и интересам государства и общества.

К.Д. Рыдченко пишет: «Указанная дефиниция не соответствуют определению цензуры, которое дано в статье 3 Закона РФ от 27 декабря 1991 г. № 2124 «О средствах массовой информации»: «цензура, то есть требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме

случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей». Иными словами, закон о СМИ запрещает только предварительную цензуру» [60, с. 41].

Интересные выводы присутствуют в работе К.Д. Рыдченко, посвященной проблеме обеспечения информационной безопасности детей в связи с принятым Федерального законом «О защите детей от информации, причиняющей вред их здоровью и развитию» [91]. При этом особое внимание автор обращает на необходимость легального закрепления процедуры отнесения информации к вредоносной [61, с. 43].

Анализ научных работ по проблеме обеспечения информационной безопасности подрастающего поколения показывает, что сфера образования и воспитания требует пристального внимания и детального правового регулирования.

Особую значимость необходимости уточнения ключевых дефиниций придает возраст потенциальных жертв правонарушений в сфере информационной безопасности (дети и молодежь). Так К.Д. Рыдченко обращает внимание на отсутствие единого легально закрепленного аппарата в рамках рассматриваемой проблемы [61, с. 42]. Он отмечает дискуссионность легальной трактовки термина «информация, причиняющая вред здоровью и (или) развитию детей», под которой понимается информация, распространение которой среди детей запрещено или ограничено в соответствии с федеральным законом о защите детей [61, с. 42].

И.И. Тазин предлагает расширить трактовку понятия информационной безопасности до информационно-психологической безопасности. Под последней он понимает «состояние защищенности психики ребенка от воздействия деструктивных информационных программ, причиняющих вред его здоровью и (или) физическому, психическому, духовному, нравственному развитию» [69, с. 222]. При этом он считает, что «предметом оценки в этом случае могут выступать телепередачи, телешоу, документальные фильмы,

художественные фильмы, мультипликационные фильмы, книги, газеты, журналы, компьютерные игры, интернет-ресурсы» [69, с. 222].

В данном случае представляется важным указание на необходимость проведения психолого-лингвистической экспертизы в каждом отдельном случае, что поможет избежать избыточного нормативного регулирования в отношении производства и распространения информации предположительно деструктивного характера.

В то же время нельзя уйти от некоторой формализации такого термина как «духовность», который является определяющим для правовой дефиниции «духовно-нравственные основы». Как отмечает А.В. Андреева, «…духовность – это сложно конструированное психологическое явление, относящееся к ценностно-смысловой сфере человека, определяющей содержание и направленность его жизни в пространственно-временной плоскости» [5, с. 25].

Понятие «духовность» исторически тесно связано с процессом воспитания. Согласно п. 2 ст. 2 ФЗ «Об образовании в Российской Федерации» [92] воспитание – это деятельность, направленная на развитие личности, создание условий для самоопределения и социализации обучающегося на основе социокультурных, духовно-нравственных ценностей и принятых в обществе правил и норм поведения в интересах человека, семьи, общества и государства.

Стратегия развития воспитания в Российской Федерации на период до 2025 года [57] рассматривает воспитание как стратегический общенациональный приоритет, требующий консолидации усилий различных институтов гражданского общества и ведомств на федеральном, региональном и муниципальном уровнях.

В контексте вышеизложенного следует отметить проблему разработки дефиниции понятия «информационное оружие». Данная дефиниция до настоящего времени вызывает различное отношение к ней у исследователей. Как отмечает А.Я. Капустин, «иными словами, ИКТ в данном контексте

выступают в качестве средства ведения военных действий (оружия)» [28, с. 92].

К.Ю. Чугунова справедливо обращает внимание на отсутствие легального определения понятия «информационное оружие»: «разве информационное оружие не поражает цель, будь то техническое средство, технологическая система или человек? Представляется, что с учетом динамики развития общества и требований актуализации законодательства в настоящее время целесообразно указание в данном Законе об оружии на такой вид оружия, как информационное» [94, с. 60].

В результате К.Ю. Чугунова предлагает следующие признаки информационного оружия: «причиняет вред здоровью чел**о**века; блокирует на неосознаваемом уровне свободу волеизъявления человека, искусственно прививает ему синдром зависимости; ведет к утрате способности к политической, культурной, нравственной самоидентификации человека; манипулирует общественным сознанием; разрушает единое информационное и духовное пространство Российской Федерации, традиционные устои общества и общественной нравственности, а также нарушает иные жизненно важные интересы личности, общества и государства» [94, с. 63].

При всем уважении к качественному анализу и выработке конкретных рекомендаций, проведенных К.Ю. Чугуновой, нельзя не высказать опасение относительно теоретической возможности признания в качестве информационного оружия человека. Это не только может привести к ущемлению ряда прав и свобод человека, но и создать правовую основу для резкого усиления репрессивных мер в отношении лиц, в силу своей профессии призванных оказывать психологическое воздействие (воспитатели, педагоги, актеры, представители творческих профессий).

Таким образом, под информационным оружием следует понимать совокупность информационно-коммуникационных технологий и цифрового контента, которые используются в качестве средства воздействия на лицо (группу лиц), а также на подрастающее поколение с целью разрушения

российских традиционных духовно-нравственных основ, а также нанесение вреда физическому и психическому здоровью и развитию.

Федеральные государственные органы надзора по обеспечению информационной безопасности действуют в соответствии с федеральным законодательством и, в частности, в соответствии с ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Приказом Минкомсвязи России утвержден порядок проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей [52]. Результаты экспертизы, оформленные в виде экспертных заключений, размещены на официальном сайте Роскомнадзора.

К сожалению, практика демонстрирует невысокий уровень эффективности данных мероприятий. Например, экспертное заключение №2/17 от 18.12.2017 г. по поводу телепередачи «Орел и решка. Рай и ад», в которой демонстрируются эпизоды с поеданием собак в южно-корейском городе Пусан, прямо указывает на необходимость запрещения демонстрации видеоряда, который может вызвать у детей страх, ужас или панику [96]. В то же время в качестве выводов в экспертном заключении присутствует лишь указание на несоответствие данного видеофильма маркировке информационной продукции 16+ [12]. Как итог экспертизы – «продукция должна иметь маркировку 18+, так как содержит информацию, не допустимую для показа подросткам».

Другими словами, в соответствии с ч. 3 ст. 5 ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» демонстрация данной передачи может быть ограничена, но не запрещена. Очевидно, что на практике, то есть в процессе домашнего просмотра, осуществить недопущение (запрет) на демонстрацию этого фильма не представляется возможным. Данный информационный знак лишь предупреждает родителей или иных лиц, несущих ответственность за детей, о вредном для психического здоровья содержании передачи. Эффективность правового регулирования здесь

недопустимо низка. Тем более, что фильм выложен в свободном доступе на официальном сайте телеканала «Пятница».

ФЗ «Об образовании в Российской Федерации» предусмотрен государственный контроль в сфере образования. Данный вид контроля, прежде всего, относится к такому показателю как «качество образования» (ст. 93). Под качеством образования понимается «комплексная характеристика образовательной деятельности и подготовки обучающегося, выражающая степень их соответствия федеральным государственным образовательным стандартам, образовательным стандартам, федеральным государственным требованиям и (или) потребностям физического или юридического лица, в интересах которого осуществляется образовательная деятельность, в том числе степень достижения планируемых результатов образовательной программы» (п. 29 ст. 2).

Обращает на себя внимание такая первостепенная характеристика качества образования как «соответствие федеральным государственным образовательным стандартам». Другими словами, качественное образование – то, которое в наибольшей степени соответствует образовательным стандартам. Представляется, что данные характеристики интеллектуальной деятельности обучающегося также самым прямым образом связаны с понятием «качество образования». При этом очевидно, что педагогические работники, да и образовательные учреждения в целом, ориентированы на исполнение положения о соответствии ФГОСам более, чем на развитие у обучающихся творческих способностей и познавательной активности, поскольку последние в меньшей степени подлежат государственному контролю, а, следовательно, от них в меньшей степени зависит оценка работы коллектива или организации.

С другой стороны, сегодня в России создана и действует разветвленная система контроля и надзора в сфере образования. Федеральная служба по надзору в сфере образования и науки [48] осуществляет руководство следующими подведомственными учреждениями.

Во-первых, это ФГБНУ «Федеральный институт педагогических измерений» (ФИПИ). ФИПИ был создан для содействия Рособрнадзору в части организации научно-методического обеспечения контроля качества подготовки обучающихся и выпускников в соответствии с федеральными государственными образовательными стандартами, разработке контрольных измерительных материалов, формированию и ведению информационных ресурсов.

К основным направлениям деятельности ФИПИ обеспечение информационной безопасности относится только в части реализации принципа законности и соблюдения установленных законом мер по оценке качества образования. Так, в Отчете за 2021 год присутствует указание на соблюдение условий информационной безопасности при подготовке к ЕГЭ 2021 года. В 2021 г. среди приказов, изданных ФИПИ, присутствовали приказы, в том числе, об утверждении регламента реагирования на инциденты информационной безопасности в информационных системах персональных данных, а также инструкции по обеспечению информационной безопасности разработок КИМ ЕГЭ. В результате деятельность института ФИПИ была признана успешной по всем направлениям [41]. Обращает на себя внимание лишь то, что изучение документов ФИПИ демонстрирует отсутствие прямых указаний на взаимосвязь таких факторов как информационная безопасность и качество образования. Единственное направление обеспечения информационной безопасности – недопущение утечки заданий ЕГЭ до его начала.

Кроме названных организаций особое внимание в контексте исследуемой проблемы привлекает Федеральное государственное бюджетное учреждение «Федеральный институт оценки качества образования» [53] Главной целью института является обеспечение информационно-аналитического и методического сопровождения исследований качества образования всех уровней. Для достижения цели институт проводит мониторинг качества образования, исследования в области

профессионального образования, принимает участие в диагностических процедурах образовательных достижений.

Постановлением Правительства Российской Федерации от 26.12.2017 г. № 1642 была утверждена государственная программа «Развитие образования» [47].

Проблема информационной безопасности детей стала предметом специальных парламентских слушаний «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве». По результатам слушаний было решено провести во всех образовательных организациях Российской Федерации «Единый урок» по безопасности в сети Интернет.

Представляется, что излишняя активность в образовании детей с помощью интернет-уроков (даже если это урок, посвященный обеспечению безопасности) не обеспечивает адекватного обыденным потребностям запроса на пользование интернетом со стороны детей. В данном случае существует опасность постепенного замещения компьютерной грамотности компьютерной зависимостью, а обучение совершению безопасных покупок в интернет-магазинах вообще выглядит как реклама.

Не претендуя в рамках данной работы на всеобъемлющий характер анализа формальных характеристик качества образования, можно сделать следующие выводы:

- методы правового регулирования, предусматривающие ограничение распространения информации, могущей нанести вред физическому и психическому здоровью детей, путем проставления информационных знаков о возрастных ограничениях, демонстрируют низкую эффективность;
- обращает на себя внимание несоответствие масштабности, разветвленности организационно-правовых форм повышения качества образования и самого качества образования;

– понятие «качество образования» не включает в себя такую составляющую как «духовно-нравственные основы»;
– необходима разработка методики и правового обеспечения проведения педагогической (психолого-педагогической) экспертизы не только в отношении проектов нормативных правовых актов и нормативных правовых актов (как предусмотрено ст. 94 ФЗ «Об образовании в Российской Федерации»), но и образовательных технологий, могущих нанести вред качеству образования и воспитания.

Далее, следует рассмотреть органы управления в сфере образования субъектов Российской Федерации как элемент системы обеспечения информационной безопасности

В структуре Министерства образования и науки Самарской области [49] находятся несколько подразделений, деятельность которых так или иначе связана с проблемой обеспечения информационной безопасности и качества образования. Одним из таких подразделений является Управление по контролю и надзору в сфере образования, которое реализует переданные полномочия Российской Федерации в сфере образования. Поскольку данная деятельность Управления осуществляется в соответствии с федеральным законодательством, а последнее не включает в себя четко сформулированных императивных норм по обеспечению информационной безопасности (за исключением технического обеспечения защиты от утечки или несанкционированного использования информации), трудно говорить о реальных практических шагах управления в данной области. Тем не менее, нужно отметить, что отсутствие активной административной работы в области защиты от деструктивного воздействия на молодежь цифровых средств получения информации частично компенсируется организацией системы дополнительного образования и воспитания детей.

Дополнительное образование и воспитание детей резонно рассматривается как «важнейшая составляющая единого образовательного

пространства, как образование, органично сочетающее в себе воспитание, обучение, творческое развитие, профессиональное самоопределение ребенка». Именно дополнительное образование «влияет на качество жизни, так как приобщает молодых людей к здоровому образу жизни, раскрывает творческий потенциал личности, побуждает к достижению общественно значимого результата».

В Самарской области реализуется государственная программа «Развитие образования и повышение эффективности реализации молодежной политики в Самарской области» на 2015 - 2030 годы» [50] одной из ведущих задач которой является совершенствование форм и методов воспитания. В каком направлении должно осуществляться совершенствование форм и методов воспитания – программа не конкретизирует. Вообще Программа насыщена общими дефинициями (совершенствование, расширение, охват), за которыми трудно увидеть реальное наполнение такого важного элемента как «качество образования». При этом авторы программы не без иронии отмечают: «Развитие региональной системы оценки качества образования не должно привести к росту контроля и бюрократии в системе образования. Этот риск может стать серьезной проблемой при использовании данных для улучшения работы организаций образования». Внятное определение термина «качество образования» отсутствует.

Такое положение позволяет сделать вывод о том, что региональные органы управления и контроля в сфере образования и воспитания не устанавливают негативной взаимосвязи между такой характеристикой образования как качество и использованием таких средств обучения как цифровые. Следуя в русле общих тенденций, рассматриваемые программные документы априори основываются на презумпции позитивного влияния цифровых средств обучения на качество образования.

Для оценки качества образования в Самарской области создан Центр мониторинга качества образования. Функционирование Центра направлено, в основном, на сбор и анализ информации о проведенных тестах, проверках,

мониторинге и т.д. Другими словами, Центр интересует не разработка методов повышения качества образования, а констатация динамики его развития.

Обеспечение информационной безопасности в сфере образования и воспитания организациями, осуществляющими образовательную деятельность. Как отмечает А.В. Андреева, «…психологическая безопасность образовательной среды предполагает такое выстраивание отношений в системе «специалисты образования – обучающиеся – образовательная программа», которая соответствует следующим критериям: отсутствие деструктивного посягательства на подсознательное, удовлетворенность межличностным общением, отсутствие препятствий для личностного роста, психологическое здоровье включенных в систему участников» [5, с. 24].

При этом главным вопросом является формирование образовательной информационной среды. Именно эта среда в значительной степени «насыщает» обучающегося информацией. Данная информация относится не только непосредственно к предмету обучения, но и к повседневной, внеурочной деятельности студента в рамках учебного заведения.

Интересные выводы по этому поводу приводит в своей работе А.В. Андреева: «В целом анализ связи направления обучения и степени проявления различных компонентов духовности не позволил нам констатировать влияния обучения на развитие духовности. Сами студенты при обсуждении полученных результатов эмпирического исследования пояснили данный вывод тем, что на развитие духовности влияет главным образом не направление обучения (психологическое, юридическое, физико-математическое), а специфика его организации» [5, с. 28].

Это очень важный и симптоматичный вывод. По сути, автор констатирует отсутствие взаимосвязи между процессом обучения (нахождения обучающегося в информационной образовательной среде ВУЗа) и ростом их духовного потенциала. С другой стороны, важным аспектом этого вывода является указание на преимущественное влияние на данные процессы не столько содержания, сколько формы его организации и подачи.

Цифровизация процесса образования является здесь одним из основных компонентов «ухода» образования в сторону от традиционных «гуманитарных» технологий. Это, в свою очередь, и приводит к снижению духовно-нравственного потенциала обучающихся, который приобретается и развивается только в общении непосредственно с людьми, а не с техническими средствами. Снижается и качество образования, если под ним понимать, помимо чисто технических, еще и гуманитарные аспекты.

Неоспорим факт определенного позитивного влияния электронных видов обучения на развитие личности. Это относится и к проблеме социализации личности, и к освоению технологии быстрого доступа к информации. Но эти технологии, как справедливо отмечает Б.У. Хашагульгов, «весьма условно защищены от антинаучной, антидуховной, заведомо ложной и просто некачественной, неграмотно преподнесенной информации» [93, с. 145].

В связи с этим Б.У. Хашагульгов видит проблему в том, «как обеспечить стабильное поступление к обучающемуся – реальному и потенциальному пользователю ПК – позитивного познавательного материала, адекватного безопасности общества, личности, государства?» [93, с. 145].

Данная проблема представляется еще более сложной. Дело в том, что современные вузы находятся в рамках наиболее востребованных со стороны обучающихся тенденций. Даже определение «качество образования» включает в себя такой критерий как соответствие «…требованиям и (или) потребностям физического или юридического лица, в интересах которого осуществляется образовательная деятельность (ст. 29 ФЗ «Об образовании в Российской Федерации»). Стоит ли говорить, что с точки зрения социологии наиболее востребованными будут именно наиболее легкие для освоения методы и технологии обучения. К сожалению, современная вузовская образовательная среда в значительной мере способствует формированию именно таких «облегченных» компонентов образовательной системы.

## 3.2 Основные направления обеспечения информационной безопасности в сфере образования и воспитания

Современное образование практически не мыслится уже без применения цифровых компонентов. В работе О.В. Насс электронные образовательные ресурсы трактуются как «компьютерные средства, которые могут быть спроектированы и использованы педагогами для достижения целей обучения» [38, с. 110]. Инновационные процессы в образовании носят объективный и, пожалуй, необратимый характер. В то же время неоправданно низким остается уровень критического отношения к результатам использования инновационных технологий. Исследователи неоднократно обращали внимание на необходимость более вдумчивого анализа и прогнозирования, в первую очередь, возможных негативных последствий неограниченного применения электронных средств обучения.

Е.А. Акользина, проанализировав работы специалистов в вопросе применения электронных средств обучения, выделила ряд существенных, по ее мнению, недостатков [2, с. 96].

А.Г. Колгатин называет одним из деструктивных факторов цифрового контента наличие в нем ошибок. Он пишет: «информационный продукт со значительным количеством ошибок представляет опасность для других участников учебного процесса. Даже человек с высоким уровнем критического мышления и предметной подготовки не всегда готов заметить ошибку в приведенных фактах или искривление значимости тех или иных аспектов проблемы. Ошибка в учебных материалах усваивается на уровне подсознания и приводит к подмене информации на уровне учебных достижений обучаемого. Более того, когда состав учебных групп неоднородный по социально-этическим взглядам, возможно навязывание определенных идей той частью группы, которая многочисленнее или более активна. Никакие технические средства не снижают указанную информационную угрозу» [31, с. 419].

Все указанное относится, в первую очередь, к сетевым формам обучения, при которых непосредственный контакт обучающегося с преподавателем сведен к минимуму, а образовательная информация доступна обучающемуся лишь в опосредованной, цифровой форме.

А.Г. Колгатин предлагает создавать новую дидактику, которая смогла бы скорректировать методы сетевого обучения и минимизировать информационные угрозы: «Необходимо совершенствовать методику преподавания дистанционных курсов на основе глубоких психолого-педагогических исследований. Это новая дидактика, которая существенно отличается от традиционной. Очень важно обеспечить на уровне школьного образования формирование информационной культуры в обществе и компетентности относительно информационного поиска» [31, с. 424].

К сожалению, подобные призывы остаются во многом не воспринятыми не в последнюю очередь потому, что такая форма обучения становится все более коммерчески привлекательной для высших учебных заведений. Но применение инновационных технологий не должно нарушать норм, охраняющих здоровье обучающихся.

Анализ нормативного материала, регулирующего организацию электронного обучения в вузе, показывает, что:

- электронное образование – одна из возможных форм организации обучения;
- для образовательных организаций, реализующих образовательные программы в сфере высшего образования, допускается применение исключительно электронного обучения;
- организация образовательного процесса регламентируется локальными нормативными актами образовательной организации, которые должны предусматривать возможность реализации ДПП в сетевой форме;

– существующие социально-экономические условия диктуют образовательным организациям необходимость расширения применения средств электронного обучения;
– не установлена взаимосвязь категорий «дистанционные образовательные технологии, электронное обучение» и «вред физическому или психическому здоровью», по умолчанию предполагается, что электронное обучение не наносит вреда физическому и психическому здоровью обучающегося;
– определение «информационная безопасность», по большей части, относится к безопасности объекта информатизации (электронного ресурса) от несанкционированного воздействия извне и в меньшей степени к безопасности субъекта информатизации (в данном случае обучающегося).

В современных научных исследованиях роль электронных средств обучения оценивается неоднозначно. При этом необходимо отметить, что не только содержание, но и сама форма работы с электронными ресурсами является потенциально деструктивным фактором, способным нанести вред психическому здоровью пользователя. Не случайно, что Всемирная организация здравоохранения (ВОЗ) признала интернет-зависимость психическим расстройством и включила эту болезнь в новую редакцию Международной классификации болезней (МКБ-11). По данным психологов, такой диагноз смогут ставить зависимым от селфи, онлайн игр, SMS и соцсетей [20].

Но уже сейчас общество, граждане, все заинтересованные лица могут сформировать свое отношение к проблеме, призвать экспертное сообщество и уполномоченные органы и организации создать эффективную систему правового регулирования отношений в сфере распространения электронного контента и ограничить его деструктивное влияние на молодежь.

С другой стороны, существует устойчивая тенденция к расширению в сфере образования применения электронного и дистанционного обучения и

снижения вплоть до полного исключения аудиторной (контактной) работы преподавателя с обучающимся.

Это в определенном смысле снимает ответственность с вузов, частично решает проблемы материального обеспечения, но не снимает вопрос о безопасности пользователя. Ответственность полностью ложится на него, поскольку режим его личной работы с компьютером ограничен лишь его собственными представлениями о вреде, наносимом цифровыми средствами обучения.

Учитывая гуманистический характер образования, его определение как «единого целенаправленного процесса воспитания и обучения» в целях, в том числе, «духовно-нравственного, творческого, физического и (или) профессионального развития человека», принцип свободы выбора получения образования согласно склонностям и потребностям человека, который, в частности, предусматривает предоставление права выбора форм получения образования, можно говорить о необходимости дополнительного правового регулирования реализации образовательных программ с помощью электронного обучения, в том числе и с помощью локальных нормативных правовых актов, принимаемых в организациях, осуществляющих реализацию образовательных программ. Необходимо обосновать альтернативность и равнозначность наряду с цифровыми, инновационными и традиционных способов получения образования.

Важным направлением развития информационного обеспечения информационной безопасности в сфере образования, является обеспечение безопасности от угроз, связанных с фальсификацией истории, так как одним из элементов системы самодезориентации общества является трансформация его культурно-исторического кода, организуемая извне.

Одной из форм (не правовых) противодействия фальсификации отечественной истории и сохранения традиционных российских духовно-нравственных ценностей стал масштабный проект «Россия – моя история».

Мультимедийный исторический парк «Россия – моя история», выросший из выставок, посвященных основным событиям российской истории, вызывает сегодня неподдельный интерес и разнообразное, в том числе объяснимо критическое, отношение в самых широких слоях общества. По целому ряду параметров (формальных и содержательных) этот парк можно с уверенностью назвать уникальным – ничего подобного в отечественном историческом научно-образовательном пространстве ранее не было [25].

Именно этот парк стал камнем преткновения в разгоревшейся дискуссии по поводу интерпретации событий отечественной истории. Сама по себе дискуссия продемонстрировала всю сложность, и честно сказать, бесперспективность решения данной проблемы. По крайней мере, в ближайшем будущем.

Несмотря на то, что материалы к проекту готовили профессиональные историки были использованы ранее не опубликованные материалы центральных архивов, в среде профессионалов и общественности нередко раздаются критические отзывы о выставке.

Теперь несколько слов о формах, которые используются для фальсификации истории. Как отмечает А.В. Казаков, «идеологическая обработка населения России из-за рубежа идет по несколько иным направлениям… В частности, например, в последние десятилетия значительный импульс получили попытки фальсификации хода и итогов Второй мировой войны, целью которых является не только умаление роли и значения СССР в победе над нацизмом, но и возложение на него, а, следовательно, и на Российскую Федерацию как его правопреемницу, ответственности за начало Второй мировой войны и последовавшего вслед за ее окончанием биполярного противостояния [26, с. 9].

Как отмечал еще в 2010 г. известный политолог С.А. Марков, «самый главный метод борьбы с фальсификациями – тщательная разработка собственной истории. Мы не можем не видеть, что система поддержки исторической науки, которая сама по себе не может быть рыночной, должна

основываться на государственной поддержке. Историки должны иметь возможность печатать книги, журналы, проводить конференции, приглашать заинтересованных людей на эти конференции, сами должны иметь возможность ездить на конференции, отстаивать на них наши позиции».

Сказанное выше – прерогатива государства и суть его политическая воля. Данные аспекты проблемы лежат вне предметного поля данной работы.

Одним из перспективных и насущных направлений правового обеспечения национальной безопасности является разработка норм, защищающих от размывания (снижения влияния на социальное поведение) традиционных российских духовно-нравственных ценностей.

Статья 78 Стратегии национальной безопасности определяет, что «к традиционным российским духовно-нравственным ценностям относятся приоритет духовного над материальным, защита человеческой жизни, прав и свобод человека, семья, созидательный труд, служение Отечеству, нормы морали и нравственности, гуманизм, милосердие, справедливость, взаимопомощь, коллективизм, историческое единство народов России, преемственность истории нашей Родины».

Стратегия развития воспитания в Российской Федерации на период до 2025 года в качестве приоритетной задачи определяет «развитие высоконравственной личности, разделяющей российские традиционные духовные ценности, обладающей актуальными знаниями и умениями, способной реализовать свой потенциал в условиях современного общества, готовой к мирному созиданию и защите Родины».

К духовно-нравственным ценностям Стратегия развития воспитания относят следующие: «человеколюбие, справедливость, честь, совесть, воля, личное достоинство, вера в добро и стремление к исполнению нравственного долга перед самим собой, своей семьей и своим Отечеством».

Соответственно общество сегодня находится на таком уровне духовно-нравственного развития, который уже с необходимостью и остротой требует

нормативного правового регулирования тех аспектов жизни общества, которые еще не так давно успешно регулировались нормами морали.

А.Н. Привалов и Ю.И. Богатырева обращают внимание на масштабы деструктивного воздействия распространения цифровых технологий в среде подрастающего поколения [51, с. 427].

Трудность обеспечения безопасности традиционных духовно-нравственных ценностей связана с невозможностью полноценного и эффективного регулирования с помощью правовых норм сферы общественной морали и нравственности. Традиционные ценности потому и традиционны, что они формировались веками, складывались исторически.

Регулирование здесь возможно не «постфактум», а превентивно с помощью воспитания и образования.

Тем не менее, некоторые меры вполне возможно реализовать.

Во-первых, при анализе ФЗ «О защите детей от информации, причиняющей вред здоровью и (или) их развитию», исследователи выделяют следующие признаки вредной для детей информации:

- побуждает к причинению вреда своему здоровью, жизни;
- провоцирует безнравственное поведение;
- отрицает семейные ценности;
- вредит правовому воспитанию;
- вызывает страх, ужас, панику;
- вызывает интерес к сексу;
- ее разглашение ущемляет права и законные интересы другого несовершеннолетнего;
- вредит половому воспитанию детей [17, с. 5].

Таким образом, из всего спектра духовно-нравственных ценностей, фигурирующих в Стратегии национальной безопасности и Стратегии воспитания, Федеральный закон защищает от посягательства (отрицания) только семейные ценности. Очевидно, что это не охватывает всего спектра негативной информации, которая способна размывать духовно-нравственную

основу российского общества. К тому же дефиниция «семейные ценности» также требует легального определения.

Во-вторых, в условиях информационно ориентированного общества серьезное деструктивное влияние на размывание традиционных российских духовно-нравственных ценностей оказывают компьютерные игры. Именно на этот аспект нам бы хотелось обратить внимание.

Современные исследователи занимают довольно критическую позицию в отношении компьютерных игр и их влияния на развитие психики и поведенческих реакций молодого поколения [68, с. 107].

Система многократного повторения определенных действий (алгоритм), которая является основой компьютерных игр, образует, по мнению авторов, «рефлекторную дугу», как у собак И.П. Павлова, что многократно усиливает эффект внушаемости и воздействия на систему ценностей игрока [68, с. 107].

Особое внимание авторы обращают на критический уровень воздействия игр на психику подрастающего поколения: «Необходимо понимать, что деструктивное влияние на психику выражается в каждодневном проявлении агрессии в коридорах школы, института, на улице и т.д. Влияние подобных компьютерных игр – более тихий, но мощный механизм по перекройке сознания наших детей» [68, с. 107].

Как кому-то ни покажется несерьезным, но именно компьютерная игра приобретает сегодня характер угрозы национальной безопасности в информационной сфере.

В-третьих, проблема размывания традиционных духовно-нравственных ценностей должна рассматриваться в контексте использования информационного оружия с целью нанесения вреда национальной безопасности Российской Федерации. В настоящей работе хотелось бы отметить, что пока идут теоретические дискуссии (безусловно, необходимые) о сущности данной дефиниции, информационное оружие в полной мере используется против населения России. Молодежь становится объектом

применения информационного оружия и трансформации духовно-нравственных ценностей с целью политического воздействия на Российскую Федерацию.

Исследователи неоднократно отмечали наличие прямой взаимосвязи изменения ценностных установок молодежи и подготовки так называемых «цветных революций» [37, с. 64].

Таким образом, анализ научной литературы и нормативного материала позволяет сделать вывод: основное внимание сконцентрировано на изучении деструктивного воздействия на молодежь содержания электронного контента. Значительно меньшее внимание уделяется форме получения и распространения информации. Критичность ситуации требует серьезного пересмотра такого подхода.

Выводы по третьей главе выпускной квалификационной работе.

Во-первых, проблема нормативного ограничения возможности получения и использования детьми и подростками информации негативного, деструктивного, пагубного характера связана с ценностными установками, отраженными в основных законах большинства европейских государств. Такие постулаты современной демократической либеральной правовой парадигмы как отсутствие цензуры в значительной мере затрудняют правовое регулирование в части защиты детей от вредной информации. При этом правовое регулирование, предусматривающее ограничение распространения информации, могущей нанести вред физическому и психическому здоровью детей, путем проставления информационных знаков о возрастных ограничениях, демонстрирует низкую эффективность.

Во-вторых, с целью противодействия снижению уровня информационной безопасности необходимо выявить и научно обосновать наличие взаимосвязи между применением цифровых средств обучения качеством образования. Необходима разработка методики и правового обеспечения проведения педагогической (психолого-педагогической)

экспертизы не только в отношении проектов нормативных правовых актов и нормативных правовых актов (как предусмотрено ст. 94 Федерального закона «Об образовании в Российской Федерации»), но и образовательных технологий, могущих нанести вред качеству образования и воспитания. Учитывая опасность излишней формализации дефиниции понятия «духовно-нравственные основы» представляется важным указание на необходимость проведения психолого-лингвистической экспертизы в каждом отдельном случае, что поможет избежать избыточного нормативного регулирования в отношении производства и распространения информации, избежать цензуры.

# Заключение

Подводя итог изложенному в настоящей выпускной квалификационной работе, необходимо обобщить выводы и вынести предложения.

Во-первых, информационная безопасность является составной частью системы национальной безопасности Российской Федерации и представляется состояние определенного объекта и деятельность, направленную на организацию обеспечения состояния защищенности данного объекта.

Угроза безопасности информации – это потенциальная возможность нарушения основных качественных характеристик (свойств) информации: конфиденциальности, целостности и доступности – при ее обработке техническими средствами. Таким образом, понятие «угроза» заключается в образовании каких-либо обстоятельств, условий, процессов, влияющих на информацию, имеющую определенную сущность. Угроза информации может возникнуть по вполне определенным причинам (факторам). Множество факторов опасности (причин возникновения угроз) можно свести в три основных группы:

- природные факторы, вызываемые физическими воздействиями стихийных природных явлений. Названные факторы в большинстве случаев неявно зависят или вообще не зависят от деятельности человека;
- технические факторы, опосредованно зависящие от деятельности человека, хотя сбои в работе оборудования и пропадания энергопитания могут быть вызваны целенаправленно;
- социальные факторы, обусловленные происходящими в обществе экономическими, политическими, нравственными изменениями и проявляющиеся в виде ошибок пользователей, несанкционированных действий обслуживающего персонала и несанкционированного воздействия на ресурсы информационных систем как со стороны своих сотрудников (внутренний нарушитель), так и посторонними

лицами (внешний нарушитель), либо теми и другими, действующими в сговоре. Данные факторы непосредственно зависят от деятельности человека.

Во-вторых, нормативно-правовые основы обеспечения информационной безопасности можно разделить на документы концептуального уровня, федеральное законодательства и другие нормативно-правовые акты. К документам концептуального уровня относится, прежде всего, Конституция Российской Федерации, Доктрина информационной безопасности, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. Важное значение для обеспечения информационной безопасности имеют федеральные законы, а также указы Президента РФ, помимо, приведенных выше, имеющих стратегическое и концептуальное значение.

В-третьих, целесообразно выделить в законодательных и плановых документах понятие «цифровые технологии», как самостоятельный предмет регулирования, что обеспечит выделение развития цифровых технологий в самостоятельное направление, а также позволит создать нормативную основу регулирования на ближайшие несколько лет, когда инструменты цифровых технологий будут в некоторой степени непредсказуемо изменять окружающую действительность.

В-четвертых, общее направление развития цифрового обеспечения должно включать следующее: постепенную интеграцию информационного пространства публичной и частной сферы; разработка инструментов и технологий для разграничения объема полномочий пользователей и обеспечения мониторинга их активности; преобладание в сфере управления программ с открытым кодом, что обеспечит постоянное выявление недостатков и их устранение и совершенствование цифровых инструментов. Также представляется важным транслирование опыта в другие регионы, что обеспечит постепенное слияние региональных информационных систем.

Благодаря этому будет облегчен сбор массива данных, их аналитическая обработка и принятие на их основе решений регионального и федерального уровня.

В-пятых, проблема нормативного ограничения возможности получения и использования детьми и подростками информации негативного, деструктивного, пагубного характера связана с ценностными установками, отраженными в основных законах большинства европейских государств. Такие постулаты современной демократической либеральной правовой парадигмы как отсутствие цензуры в значительной мере затрудняют правовое регулирование в части защиты детей от вредной информации. При этом правовое регулирование, предусматривающее ограничение распространения информации, могущей нанести вред физическому и психическому здоровью детей, путем проставления информационных знаков о возрастных ограничениях, демонстрирует низкую эффективность.

В-шестых, можно вынести следующие направления обеспечения информационной безопасности в сфере образования и воспитания.

В сфере образования:

- с целью противодействия снижению уровня информационной безопасности необходимо выявить и научно обосновать наличие взаимосвязи между применением цифровых средств обучения качеством образования;
- необходима разработка методики и правового обеспечения проведения педагогической экспертизы не только в отношении проектов нормативных правовых актов и нормативных правовых актов, но и образовательных технологий, могущих нанести вред качеству образования и воспитания;
- дефиниция «качество образования» требует уточнения и соотнесения его с категорией «духовно-нравственные ценности». Для этого необходимо внести изменения в ряд федеральных законов, в частности в Федеральный закон «Об образовании в Российской

Федерации» и исключить из него определение образования в Российской Федерации как «услуги».

В сфере воспитания:

- в условия информационных войн традиционные духовно-нравственные ценности, исторически сложившиеся в России, как основа национально-государственной идентичности, существующие в виде информации, должны рассматриваться в качестве самостоятельного объекта информационного воздействия;
- учитывая опасность излишней формализации дефиниции понятия «духовно-нравственные основы» представляется важным указание на необходимость проведения психолого-лингвистической экспертизы в каждом отдельном случае, что поможет избежать избыточного нормативного регулирования в отношении производства и распространения информации, избежать цензуры;
- существующее определение понятия «информационная безопасность», по большей части, относится к безопасности объекта информатизации от несанкционированного воздействия извне и в меньшей степени к безопасности субъекта информатизации. Очевидно, что не только содержание, но и сама форма работы с электронными ресурсами является потенциально деструктивным фактором, способным размывать традиционные духовно-нравственные ценности. Поэтому необходимо широко обсудить возможность принятия закона о возрастных ограничениях для пользователей электронных систем;
- для эффективного обеспечения информационной безопасности в сфере образования и воспитания необходимо использовать не только меры регулятивного, но и охранительного характера.

## Список используемой литературы и используемых источников


1. Авакьян С.А. Задачи конституционного права в аспекте защиты (от) информации // Конституционное и муниципальное право. 2022. № 8. С. 3 – 11.
2. Акользина Е.А. Использование электронных образовательных ресурсов в процессе обучения: достоинства, недостатки // Психолого-педагогический журнал Гаудеамус. № 2 (22), 2013. С. 96-99.
3. Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. 1999. № 1. С. 44-47.
4. Алиева М.Ф. Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2012. № 4. С. 98-102.
5. Андреева А.В. Духовность как основа технологии сопровождения образовательного процесса в целях обеспечения его психологической безопасности // Известия российского государственного педагогического университета им. А.И. Герцена. 2008. № 74(2). С. 24-28.
6. Ахмадиев Ф.В. Свобода слова и проблемы информационной безопасности общества и личности // Вестник Челябинского государственного университета. 2013. № 38 (329). Философия. Социология. Культурология. Вып. 31. С. 34-38.
7. Барков А.В., Киселев А.С. О правовом обеспечении безопасности информационно-телекоммуникационной инфраструктуры банков и государственных структур // Банковское право. 2022. № 4. С. 20 - 27.
8. Бачило И.Л. Информационное право. Основы практической информатики: учеб. пособие. М., 2003. 422 с.
9. Безугленко О.С. Вопросы правового регулирования информационной защиты несовершеннолетних в образовательном процессе // Мониторинг правоприменения. 2014. № 4 (13). С. 66-70.

10. Бекбергенева Д. Е. Управление цифровизацией социально-экономического развития региона.: Автореферат дисс. .. д-ра эконом наук. Ростов-на-Дону, 2022. 34 с.

11. Брандман Э.М. Информационная безопасность российского общества в современных условиях // Власть. 2007. № 5. С. 68-72.

12. Верютин В.Н. Административно-правовой механизм обеспечения информационной безопасности как составной части национальной безопасности // Вестник Краснодарского университета МВД России. 2009. № 1. С.137-142.

13. Вольнов Р.В. Психолого-правовые особенности обеспечения информационно-психологической безопасности личности: автореф. дис. … канд. психол. наук. М., 2011. 33 с.

14. Гаязова Л.А. Психологические основания мониторинга безопасности образовательной среды // Известия российского государственного педагогического университета им. А.И. Герцена. 2012. № 145. С. 65-68.

15. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 г. № 14-ФЗ (ред. от 01.07.2021) // СЗ РФ. 1996. № 5. Ст. 410.

16. Данилин А.В. Электронные государственные услуги и административные регламенты: от политической задачи к архитектуре «электронного правительства». М.: Инфра-М, 2014. 270 с.

17. Дорогова Е.В. Юридическая сущность информации, причиняющей вред здоровью и (или) развитию детей // Правопорядок: история, теория, практика. 2014. № 1 (2). С. 5-8.

18. Желонкин А.Д. Функция обеспечения информационного развития общества и информационной безопасности в системе функций российского государства // Вестник Саратовской государственной юридической академии. 2016. № 4(111). С. 153-156.

19. Журавлев М.С. Философия информационной безопасности // Известия Тульского государственного университета. Серия: гуманитарные науки. 2014. № 2. С.43-48.

20. Зависимость от селфи и соцсетей могут признать заболеванием Электронный ресурс: http://www.m24.ru/articles/74278?utm_source=CopyBu?utm_source=CopyBuf (дата обращения: 16.03.2023).

21. Закон РФ от 21.07.1993 г. № 5485-1 (ред. от 05.12.2022) «О государственной тайне» // СЗ РФ. 1997. № 41. Ст. 8220-8235.

22. Закон РФ от 27.12.1991 г. № 2124-1 (ред. от 29.12.2022) «О средствах массовой информации» // Российская газета. 1992. № 32.

23. Затонский А.В. Информационные технологии: разработка информационных моделей и систем. М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. С-260 с.

24. Иванцов А.М. Основы информационной безопасности. Курс лекций: учебное пособие: [в 2 частях]. Часть 1. Ульяновск: УлГУ, 2019. 72 с.

25. Исторический парк «Россия – моя история» // Электронный ресурс. URL: https://myhistorypark.ru/ (дата обращения 10.03.2023).

26. Казаков А.В. «Цветная революция» в России: миф или реальность? // Власть. 2015. № 4. С.9-12.

27. Калинченко Ю.П. Административно-правовое регулирование обеспечения информационной безопасности в интернете // Вестник Белгородского юридического института МВД России. 2014. Вып. 2(1). С.89-96.

28. Капустин А.Я. Угрозы международной информационной безопасности: формирование концептуальных подходов // Журнал российского права. 2015. № 10. С. 92-95.

29. Карминский А.М. Методология создания информационных систем: Учебное пособие. М.: ИД ФОРУМ: ИНФРА-М, 2012. 377 с.

30. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 г. № 195-ФЗ (ред. от 29.12.2022) // СЗ РФ. 2002. № 1 (Ч. 1). Ст. 1.

31. Колгатин А.Г. Информационная безопасность в системах открытого образования // Образовательные технологии и общество. 2014. Т.17. № 1. С. 418-426.

32. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный текст Конституции РФ, включающий новые субъекты Российской Федерации - Донецкую Народную Республику, Луганскую Народную Республику, Запорожскую область и Херсонскую область, опубликован на Официальном интернет-портале правовой информации http://pravo.gov.ru, 06.10.2022.

33. Копылов В.А. Информационное право. М., 2002. 512 с.

34. Крутских А.В., Зиновьева Е.С. Международная информационная безопасность: подходы России. М.: МГИМО МИД России, 2021. 266 с.

35. Люсова О.В. Психологическая безопасность образовательной среды и субъективное благополучие обучающихся // Вестник Волгоградского государственного университета. Сер.11 Естественные науки. 2015. № 2(12). С. 134-136.

36. Марков А.А. Управление процессами формирования информационной безопасности общества: социологический аспект // Вестник СПбГУ. Сер. 12. 2012. Вып. 2. С. 312-317.

37. Меркулов П.А. Молодежь как основной ресурс «цветных революций» и борьба за нее // Власть. 2015. № 6. С. 64-65.

38. Насс О.В. Формирование компетентности педагогов в проектировании электронных образовательных ресурсов в контексте обновления общего среднего и высшего образования: монография. М.: Изд-во МПГУ, 2010. 240 с.

39. Национальная программа «Цифровая экономика Российской Федерации» [Электронный ресурс] Режим доступа: http://government.ru/info/35568/ (дата обращения: 05.02.2023)

40. Открытость государства в России – 2020. URL: https://ach.gov.ru/upload/pdf/Otkrytost-2020.pdf (дата обращения: 05.03.2023).

41. Отчет о деятельности Федерального государственного бюджетного научного учреждения «Федеральный институт педагогических измерений» в 2021 году // URL: http://www.fipi.ru/sites/default/files/document/1518421390/otchet_fipi_za_2021_g.pdf (дата обращения: 16.03.2023).

42. Отчет о реализации программы «Информационное общество» [Электронный ресурс] Режим доступа: https://rospatent.gov.ru/ru/about/openrospatent/target-programs/otchet-gp-23 (дата обращения: 10.02.2023)

43. Пономарев Н.Н. Безопасность как социально-юридический феномен // Общество и право. 2011. № 4(36). С. 78-81.

44. Постановление Правительства РФ от 02.06.2008 г. № 418 (ред. от 17.12.2021) «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» // СЗ РФ. 2008. № 23. Ст. 2708.

45. Постановление Правительства РФ от 06.07.2015 г. № 676 (ред. от 23.12.2021) «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» // СЗ РФ. 2015. № 28. Ст. 4241.

46. Постановление Правительства РФ от 15.07.2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» // СЗ РФ. 2022. № 30. Ст. 5610.

47. Постановление Правительства РФ от 26.12.2017 г. № 1642 (ред. от 01.12.2022) «Об утверждении государственной программы Российской Федерации «Развитие образования» // СЗ РФ. 2018. № 1 (Ч. 2). Ст. 375.

48. Постановление Правительства РФ от 28.07.2018 г. № 885 (ред. от 25.12.2021) «Об утверждении Положения о Федеральной службе по надзору в сфере образования и науки и признании утратившими силу некоторых актов Правительства Российской Федерации» // СЗ РФ. 2018. № 32 (Ч. 2). Ст. 5344.

49. Постановление Правительства Самарской области от 20.06.2008 г. № 238 (ред. от 21.11.2022) «Об утверждении Положения о министерстве образования и науки Самарской области» // Волжская коммуна. 2008. № 152(16195).

50. Постановление Правительства Самарской области от 21.01.2015 г. № 6 (ред. от 26.12.2022) «Об утверждении государственной программы Самарской области «Развитие образования и повышение эффективности реализации молодежной политики в Самарской области» на 2015 - 2030 годы» // Волжская коммуна. 2015. № 16(29215).

51. Привалов А.Н., Богатырева Ю.И. Основные угрозы информационной безопасности субъектов образовательного процесса // Известия Тульского государственного университета. Гуманитарные науки. 2012. № 3. С. 427-433.

52. Приказ Минкомсвязи России от 29.08.2012 г. № 217 «Об утверждении порядка проведения экспертизы информационной продукции в целях обеспечения информационной безопасности детей» // Российская газета. 2012. № 245.

53. Приказ Рособрнадзора от 25.12.2015 г. № 2409 (с изм. от 15.09.2022) «Об утверждении устава федерального государственного бюджетного учреждения «Федеральный институт оценки качества образования» [Электронный ресурс] // СПС КонсультантПлюс.

54. Прончев Г.Б., Монахов Д.Н., Лонцов В.В. Безопасность виртуальных социальных сред в информационном обществе // Пространство и Время. 2013. № 4. С. 232-236.

55. Прудникова Л.Б., Шеншин В.М., Глейберман Н.С. Информация и информационная безопасность как атрибуты гражданского общества (краткий

обзор взаимосвязи) // Государственная власть и местное самоуправление. 2022. № 7. С. 7 - 9.

56. Распоряжение Правительства РФ от 22.06.2022 г. № 1661-р «Об утверждении перечня ключевых органов (организаций), которым необходимо осуществить мероприятия по оценке уровня защищенности своих информационных систем с привлечением организаций, имеющих соответствующие лицензии ФСБ России и ФСТЭК России» // СЗ РФ. 2022. № 26. Ст. 4571.

57. Распоряжение Правительства РФ от 29.05.2015 г. № 996-р «Об утверждении Стратегии развития воспитания в Российской Федерации на период до 2025 года» // СЗ РФ. 2015. № 23. Ст. 3357.

58. Распоряжение Правительства РФ от 29.12.2014 г. № 2769-р (ред. от 18.10.2018) «Об утверждении Концепции региональной информатизации» // СЗ РФ. 2015. № 2. Ст. 544.

59. Расторгуев С.П. Философия информационной войны. М., 2016. 495 с.

60. Рыдченко К.Д. «Моральный кодекс» пользователя Интернет и государственная цензура киберпространства: некоторые вопросы законодательного регулирования // Мониторинг правоприменения. 2012. № 3. С. 40-44.

61. Рыдченко К.Д. «Недетские» проблемы обеспечения информационной безопасности детей // Вестник Воронежского института МВД России. 2015. № 2. С. 43-48.

62. Рыдченко К.Д. Интересы и угрозы безопасности России в информационно-психологической сфере // Пробелы в российском законодательстве. 2009. № 4. С. 349-354.

63. Савельев А.И. Проблема информационной безопасности несовершеннолетних в сети интернет // Юридическая наука и правоохранительная практика № 2 (36) 2016. С. 62-64.

64. Смирных С.Е. Международная информационная безопасность как гарантия осуществления права народов на самоопределение // Международное право и международные организации. 2022. № 2. С. 20 - 30.

65. Соколовская С.А. Информационные технологии и информационная безопасность в государственном управлении: учебное пособие. СПб.: Изд-во СПбГЭУ, 2019. 98 с.

66. Стратегии цифровой трансформации регионов России [Электронный ресурс] Режим доступа: https://www.tadviser.ru/index.php/ (дата обращения: 05.02.2023).

67. Стрельцов А.А. Обеспечение информационной безопасности России: теоретические и методологические основы / Под ред. В.А. Садовничего, В.П. Шерстюка. М.: МЦНМО, 2002. 289 с.

68. Сысоев Ю.В., Лебедев И.Б., Филатова Т.П. Этимология создания компьютерных игр с содержанием в сюжете жестоких сцен и их метод психологического воздействия по аналогии с игровыми автоматами // Преподаватель XXI век. 2015. № 4. С. 107-110.

69. Тазин И.И. Правовое обеспечение информационно-психологической безопасности несовершеннолетних // Вестник Томского государственного педагогического университета. 2012. № 6 (121) С. 223-230.

70. Трухачева М.А. Правовое регулирование средств массовой информации в процессе социализации детей: теория и повседневная практика // Вестник Поволжского института управления. 2015. № 5(50) С. 83-88.

71. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 29.12.2022) // СЗ РФ. 1996. № 25. Ст. 2954.

72. Указ Президента РФ от 01.03.2011 г. № 248 (ред. от 06.06.2022) «Вопросы Министерства внутренних дел Российской Федерации» // СЗ РФ. 2011. № 10. Ст. 1334.

73. Указ Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // СЗ РФ. 2022. № 18. Ст. 3058.

74. Указ Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» / СЗ РФ. 2021. № 27 (Ч. II). Ст. 5351.

75. Указ Президента РФ от 03.08.2018 г. № 471 «О некоторых вопросах Межведомственной комиссии по защите государственной тайны» // СЗ РФ. 2018. № 32 (Ч. 2). Ст. 5317.

76. Указ Президента РФ от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.

77. Указ Президента РФ от 06.03.1997 г. № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» // СЗ РФ. 1997. № 10. Ст. 1127.

78. Указ Президента РФ от 07.08.2004 г. № 1013 (ред. от 03.03.2022) «Вопросы Федеральной службы охраны Российской Федерации» // СЗ РФ. 2004. № 32. Ст. 3314.

79. Указ Президента РФ от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // СЗ РФ. 2017. № 20. Ст. 2901

80. Указ Президента РФ от 09.11.2022 г. № 809 «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей» // СЗ РФ. 2022. № 46. Ст. 7977.

81. Указ Президента РФ от 10.09.2014 г. № 627 (ред. от 26.12.2022) «О Военно-промышленной комиссии Российской Федерации» (вместе с «Положением о Военно-промышленной комиссии Российской Федерации») // СЗ РФ. 2014. № 37. Ст. 4938.

82. Указ Президента РФ от 11.05.2006 г. № 473 (ред. от 24.09.2007) «Вопросы Федеральной таможенной службы» // СЗ РФ. 2006. № 20. Ст. 2162.

83. Указ Президента РФ от 12.04.2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СЗ РФ. 2021. № 16 (Ч. 1). Ст. 2746.

84. Указ Президента РФ от 16.08.2004 г. № 1085 (ред. от 08.12.2021) «Вопросы Федеральной службы по техническому и экспортному контролю» // СЗ РФ. 2004. № 34. Ст. 3541.

85. Федеральный закон от 03.04.1995 г. № 40-ФЗ (ред. от 05.12.2022) «О федеральной службе безопасности» // СЗ РФ. 1995. № 15. Ст. 1269.

86. Федеральный закон от 09.02.2009 г. № 8-ФЗ (ред. от 14.07.2022) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. 2009. № 7. Ст. 776.

87. Федеральный закон от 22.12.2008 г. № 262-ФЗ (ред. от 14.07.2022) «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // СЗ РФ. 2008. № 52 (Ч. 1). Ст. 6217.

88. Федеральный закон от 27.07.2006 г. № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (Ч. 1). Ст. 3448.

89. Федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 14.07.2022) «О персональных данных» // СЗ РФ. 2006. № 31 (Ч. 1). Ст. 3451.

90. Федеральный закон от 28.12.2010 г. № 390-ФЗ (ред. от 09.11.2020) «О безопасности» // СЗ РФ. 2011. № 1. Ст. 2.

91. Федеральный закон от 29.12.2010 г. № 436-ФЗ (ред. от 29.12.2022) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48.

92. Федеральный закон от 29.12.2012 г. № 273-ФЗ (ред. от 29.12.2022) «Об образовании в Российской Федерации» // СЗ РФ. 2012. № 53 (Ч. 1). Ст. 7598.

93. Хашагульгов Б.У. Информационная безопасность образовательного процесса в условиях трансфинитности электронного обучения // Мир науки, культуры, образования. 2010. № 4(23) С. 145-148.

94. Чугунова К.Ю. Информационное оружие как угроза национальной безопасности Российской Федерации // Актуальные проблемы российского права. 2015. № 7 (56) С. 60-64.

95. Шевко Н.Р. Актуальные проблемы обеспечения информационной безопасности современного общества // Вестник Казанского юридического института МВД России. 2012. № 8. С. 56-60.

96. Экспертное заключение №2/17 результат анализа продукции средств массовой информации, видеофильма (передачи) «Орел и решка. Рай и ад. Пусан. Южная Корея», расположенного на официальном сайте телеканала «Пятница» // Электронный ресурс: URL: https://rkn.gov.ru/docs/155237_2712201.pdf (дата обращения 15.02.2023).

97. Яблочников С.Л., Яблочникова И.О. Психологическая составляющая безопасности системы образования // Личность в меняющемся мире: здоровье, адаптация, развитие. Электронный научный журнал. 2015. № 3(10). С. 141-144.

98. Global Competitiveness Index 2017-2018. Rankings. URL: https://web.archive.org/web/20190123140620/ http://www3.weforum.org/docs/GCR2017-2018/04Backmatter/TheGlobalCompetitivenessReport2017%E2%80%932018AppendixB.pdf (дата обращения: 16.02.2023).

99. The Global Competitiveness Report 2021: official website of World Economic Forum. URL: https://gtmarket.ru/ratings/imd-world-competitiveness-ranking (дата обращения: 05.03.2023).