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 В.О. Волкова
(Инициалы Фамилия) (личная подпись)

Руководитель к.ю.н., В.В. Романова
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2024

Аннотация

Тема дипломной работы: Государственно-правовой механизм обеспечения информационной безопасности.

Информационная безопасность в современном понимании – явление относительно новое. В «доцифровую» эпоху информацию тоже необходимо было защищать от противника и от различных неблагоприятных воздействий. Однако в цифровую эпоху ситуация меняется принципиально. Важно подчеркнуть, что информационная безопасность, это не просто программы и отдельные технические продукты – это целый комплекс правовых, организационных, научно-технических, кадровых, экономических, информационно-аналитических и других мер, которые позволяют обеспечить информационную безопасность в ее современном понимании.

Объектом исследования являются общественные отношения в области обеспечения информационной безопасности.

Предмет исследования представлен массивом нормативных правовых актов, регулирующих отношения в сфере обеспечения информационной безопасности.

Целью исследования является изучение государственно-правового механизма обеспечения информационной безопасности в России.

Структура исследования обусловлена его целью и задачами. Работа состоит из введения, трех глав, разделенных на шесть параграфов, заключения, а также списка используемой литературы и используемых источников.

Оглавление

Введение

Актуальность исследования. На сегодняшний день информационные технологии проникли практически во все сферы человеческой деятельности. Без них уже невозможно представить себе медицину и образование, производство и индустрию развлечений, торговлю и логистику, финансы и государственное управление. Информационные технологии реализуются во все новых приложениях, делают возможными все новые бизнес-модели. Информационные технологии используются не только в компьютерах, но уже функционируют в повседневных предметах, причем масштабы этого явления дают повод говорить об «интернете вещей». Однако в развитии информационных технологий есть ряд отрицательных аспектов и рисков (кража данных, несанкционированный доступ, вредоносное программное обеспечение, воздействие на критическую информационную инфраструктуру и др.).

2022 год для России стал уникальным с точки зрения информационной безопасности: беспрецедентное ужесточение регуляторики в этой области, введение новых правил и требований к защите данных, рост кибератак на отечественные компании и целые отрасли экономики, дефицит специалистов в сфере обеспечения информационной безопасности, форсирование импортозамещения. Все это оказало колоссальное влияние на сферу информационной безопасности частных и государственных предприятий, общества в целом.

Согласно ежегодному отчету Центра мониторинга кибербезопасности «Лаборатории Касперского» «Managed Detection and Response» в 2023 году в России и СНГ с наибольшим числом кибератак столкнулись организации в сферах промышленности (20% от общего количества инцидентов в изучаемом регионе), финансов (17%) и информационных технологий (8%) [61].

Сегодня интерес для злоумышленников все чаще представляют такие сферы, как образование, здравоохранение, телекоммуникации. За 2023 год число инцидентов в этих отраслях выросло, причем эта же тенденция прослеживается для инцидентов высокого уровня критичности, которые хуже поддаются автоматическому реагированию и требуют оперативного вмешательства специалистов.

Тем самым, информационная безопасность в современном понимании – явление относительно новое. В «доцифровую» эпоху информацию тоже необходимо было защищать от противника и от различных неблагоприятных воздействий. Однако в цифровую эпоху ситуация меняется принципиально. Важно подчеркнуть, что информационная безопасность, это не просто программы и отдельные технические продукты – это целый комплекс правовых, организационных, научно-технических, кадровых, экономических, информационно-аналитических и других мер, которые позволяют обеспечить информационную безопасность в ее современном понимании.

Степень научной разработанности темы исследования. В исследованиях ряда ученых, таких как А.В. Федоров и В.Н. Цыгичко, информационная безопасность связывается с глобальными информационными вызовами и вопросами международной безопасности. В работах М.И. Абдурахманова, В.А. Баришполец, В.Л. Манилова, В.С. Пирумова информационная безопасность рассматривается на уровне национальной безопасности и стратегических геополитических вопросов. В работах Г.А. Атаманова, В.Н. Лопатина, А.В. Манойло, А.И. Петренко, Д.Б. Фролова информационная безопасность рассмотрена в контексте государственной информационной политики в условиях информационных войн и геополитического противостояния.

Объектом исследования являются общественные отношения в области обеспечения информационной безопасности.

Предмет исследования представлен массивом нормативных правовых актов, регулирующих отношения в сфере обеспечения информационной безопасности.

Целью исследования является изучение государственно-правового механизма обеспечения информационной безопасности в России.

Задачи исследования:

- рассмотреть подходы к определению понятия информационной безопасности;
- классифицировать и изучить современные угрозы информационной безопасности;
- провести анализ правового механизма обеспечения информационной безопасности;
- изучить компетенцию органов государственной власти в области обеспечения информационной безопасности;
- исследовать вопросы обеспечения информационной безопасности несовершеннолетних;
- провести анализ системы правового обеспечения международной информационной безопасности в условиях геополитических трансформаций.

Методологической основой исследования являются диалектический и формально-юридический методы познания. Дедуктивный метод исследования применялся для определения понятия и сущности авторских прав и их объектов. При написании работы используются логический метод и метод сравнительного анализа.

Теоретическая основа работы представлена научными трудами отечественных и зарубежных ученых, научными статьями и монографиями, диссертациями и авторефератами диссертаций, посвященных различным аспектам обеспечения информационной безопасности.

Нормативной базой исследования послужили положения нормативных правовых актов международного уровня, Конституции РФ, отечественного законодательства, регулирующего отношения в сфере обеспечения информационной безопасности и др.

Эмпирической основой исследования стали материалы исследований Фонда развития Интернет, Центра мониторинга кибербезопасности «Лаборатории Касперского», практика Региональных инновационных площадок, статистические сведения и аналитическая информация по теме работы.

Структура исследования обусловлена его целью и задачами. Работа состоит из введения, трех глав, разделенных на шесть параграфов, заключения, а также списка используемой литературы и используемых источников.

Глава 1 Понятие и угрозы информационной безопасности

1.1 Определение информационной безопасности

Привлечение внимания общественности к проблемам информационной безопасности обусловлено спецификой жизни в современном обществе. Традиционные социальные практики сокращаются, в них стремительно проникают современные информационные технологии, придавая им характер информационно-емких – в работу с информацией в данный момент вовлечена большая часть общества. Это явление подробно описывали в своих работах теоретики постиндустриального, информационного общества Ё. Масуда, Д. Белл, М. Кастельс, Э. Тоффлер и др.

В отечественной научной мысли представлен значительный потенциал различных исследований теории национальной безопасности и методологии ее практической реализации. Разработан и апробирован довольно обширный понятийный аппарат, отражающий сущность и социально-политическое содержание национальной безопасности, ее взаимообусловленность с процессами развития общества □6, с. 46□.

Безопасность следует понимать, как систему свойств, в которую входят возможные жертвы и угрозы для них. Стабильность, как и безопасность необходимый аспект для развития суверенного государства. Стабильность обеспечивает приемлемую внешнюю и внутреннюю среду для жизни. Также государство может чувствовать себя в безопасности даже при нестабильном истечение.

Основываясь на большом количестве научных публикаций, можно отметить, что есть достаточно большой интерес российских ученых к этой проблеме. Одни авторы считают, что понятие «национальная безопасность» тесно связанна с определенным потенциалом, способностью противостоять каким – либо действиям какими бы они не были и откуда бы ни исходили. Другие авторы представляют анализ национальной безопасности как некую

характеристику угроз, которые способны подорвать жизнедеятельность и развитие человека, общества и самого государства. Есть ученые, которые определяют национальную безопасность как отсутствие внешних угроз.

Эффективность системы национальной безопасности определяется тем, насколько правильно он может идентифицировать угрозы и риски. Оценка риска предполагает не только выявление интенсивности негативного воздействия факторов, но и построение его конкретных форм. Процедуры оценки основаны на выявлении негативных факторов воздействия, установлении степени их влияния на систему экономической безопасности фирмы и прогнозировании.

За последние несколько лет все популярнее стал термин «национальная безопасность государства». Причиной тому является увеличение числа внешнеполитических угроз, а также организация необходимых мер для обеспечения организационного и материального порядка.

В современном этапе развития нашего государства, национальная безопасность рассматривается как отсутствие угрозы как таковой и организация полноценной работы всех систем, с помощью которых и проводится работа по устранению этих угроз.

Таким образом, под понятием «безопасность» подразумеваются такие составляющие, как объект безопасности и угрозы, которые он представляет, субъект, определяющий безопасность объекта, а также инструменты, обеспечивающие эту безопасность в виде нормативно-правовых функций субъекта.

В качестве объекта могут выступать как иные государства, сами люди, а также что немаловажно различные объекты, занимающиеся деятельностью, которая может представлять угрозу для государства (стратегически важные объекты, энергетические объекты, природно-технические объекты). В качестве примера последних можно привести различные атомные станции, гидроэлектростанции и так далее. В случае катастрофы или

террористического захвата такого объекта гражданам может грозить опасность.

Таким образом, на современном этапе развития нашего государства, национальная безопасность рассматривается как отсутствие угрозы как таковой и организация полноценной работы всех систем, с помощью которых и проводится работа по устранению этих угроз. Таким образом, под понятием «безопасность» подразумеваются такие составляющие, как объект безопасности и угрозы, которые он представляет, субъект, определяющий безопасность объекта, а также инструменты, обеспечивающие эту безопасность в виде нормативно-правовых функций субъекта.

Большое значение национальной безопасности продиктовано преимущественно происходящими глобальными процессами, которые свойственны в современное время для общественно-экономического развития мира.

Субъектами обеспечения национальной безопасности могут выступать участники процесса, которые способны самостоятельно и свободно действовать. Следовательно, таким субъектом представляет собой само государство, которое осуществляет свои функции через законодательные, исполнительные и судебные органы власти, а также общество и население страны.

Органы законодательной власти создают законодательную базу в сфере обеспечения национальной безопасности, где они принимают решения в рамках своего ведения по проблеме использования силы и средств обеспечения безопасности, также и применение военной силы. Они вдобавок рассматривают и принимают федеральные законы по вопросам принятия и расторжение международных договоров РФ по безопасности, если они соответствуют представлениям нашей страны.

В настоящее время мы являемся свидетелями того, как смещаются акценты в трактовке характеристик современного общества – социальные процессы описываются через понятие информации [21].

Информационное общество – это социологическая и футурологическая концепция, которая рассматривает производство и использование научной, технической и другой информации как неотъемлемую часть общественного развития. Концепция информационного общества – это своего рода разновидность теории постиндустриального общества.

Общество считается информационным, если:

- «любое лицо, группа лиц или организация в любой стране и в любое время могут получать за соответствующую плату или безвозмездно на основе автоматизированных систем доступа и связи всю информацию, необходимую для их жизнедеятельности и решения личных и социально значимых задач;
- современные информационно-коммуникационные технологии создаются, эксплуатируются и доступны для всех людей, социальных групп или организаций в обществе;
- наличие развитой инфраструктуры, обеспечивающей создание национальных ресурсов данных в объеме, необходимом для поддержания постоянно ускоряющегося научно-технического и социально-исторического развития;
- происходит процесс ускоренной автоматизации и роботизации всех сфер и отраслей производства и управления;
- происходят радикальные изменения социальных структур, следствием которых оказывается расширение сферы информационной деятельности и услуг» [5, с. 9].

В Российской Федерации проблема информационной безопасности впервые была поднята в 1992 году в связи с принятием законодательных актов о правовой защите компьютерных программ.

В основе российской концепции информационной безопасности лежит представление о ней как о неотъемлемой части национальной безопасности [23]. В Доктрине информационной безопасности РФ понятие «информационная безопасность» определяется достаточно широко и

понимается как «защита личности, общества и/или государства от внутренних и внешних информационных угроз, обеспечивающая тем самым соблюдение конституционных прав и свобод, качества и уровня жизни граждан, а также суверенитет, территориальную целостность и устойчивое социально-экономическое развитие государства, его оборону и безопасность» [8]. Тем самым, данное понятие трактуется как состояние защищенности национальных интересов в информационной сфере, определяемое совокупностью сбалансированных интересов личности, общества и государства.

В Доктрине информационной безопасности РФ установлены общие принципы ее обеспечения. В частности: защита конституционных прав граждан, защита критической информационной инфраструктуры России, развитие российской науки и информационных технологий, предоставление (российскому обществу и международному сообществу) достоверной информации о национальной государственной политике и официальных позициях властей, содействие в создании международной системы информационной безопасности, защита государственного суверенитета в информационном поле.

Российские правовые нормы в области информационной безопасности распространяются на следующие области:

- специальные режимы защиты информации, требующие реализации определенных мер кибербезопасности (например, защита персональных данных или защита государственной тайны);
- ограничения для операторов связи (например, требование хранить данные о коммуникациях в течение определенного периода времени);
- требования кибербезопасности, применимые к критической информационной инфраструктуре;

– ряд статей уголовного закона России, которые де-факто вводят дополнительные ограничения (например, запрет на создание компьютерных вирусов и кибермошенничество);
– отдельные системы кибербезопасности, созданные частными компаниями, с учетом общих ограничений, предусмотренных законодательством и др.

В учебной литературе информационная безопасность рассматривается как защита информации и защита от информации [14]. При этом дифференциация информационной безопасности на указанные виды является общепризнанной в науке. К примеру, подчеркивается, что «информационная безопасность, являясь составным элементом национальной безопасности, имеет два направления: безопасность информации (защита информации) и безопасность от информации (защита от «опасной», неадекватной картине мира информации)» [33, с. 21].

В учебной литературе защита информации определяется как деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированного и непреднамеренного воздействия на нее. Таким образом, суть защиты данных заключается в выявлении, устранении или нейтрализации негативных источников, причин и обстоятельств воздействия на информацию. Эти источники угрожают безопасности данных [39, с. 25].

Защита от информации определяется через категорию информационной безопасности личности. При этом в специальной литературе нет единства в подходах исследователей к определению этого понятия. Так, к примеру, А.С. Жаров предлагает следующее определение: «информационная безопасность личности – это совокупность общественных отношений, складывающихся в процессе защиты ее конституционных прав и свобод от угроз в информационной сфере» [10, с. 15].

С.В. Нуянзин и О.С. Нуянзин предлагают учитывать сознание личности: «информационная безопасность личности – это состояние

защищенности, при котором отсутствует риск, связанный с причинением информацией вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию человека» [24].

Ю.И. Богатырева под информационной безопасностью личности понимает «состояние и условие жизнедеятельности личности, при которых отсутствует или минимизирована угроза нанесения вреда личному информационному пространству и той информации, которой обладает индивид» [3, с. 10].

Согласно И.В. Роберт «информационная безопасность личности – это защита от внешней неэтичной, нелегитимной, противозаконной, агрессивной информации; некачественной педагогической продукции, реализованной на базе информационно-коммуникационных технологий, не отвечающей педагогико-эргономическим требованиям; заимствования результатов интеллектуальной собственности, представленной в электронном виде, влекущие за собой потерю авторских прав» [34, с. 25].

Более подробная характеристика информационной безопасности личности дана в диссертации А.А. Тамодлина. По мнению автора, «информационная безопасность в широком смысле определяется как состояние, при котором отсутствует возможность причинения пользователю ущерба информацией из внешнего мира. Что касается информационной безопасности в узком значении, то это, прежде всего, состояние защищенности конституционных прав человека и гражданина на поиск, получение, передачу информации, а также защиту персональной информации и психики от негативных воздействий» [40].

Как представляется, под информационной безопасностью личности следует понимать состояние защищенности, обеспечивающее реализацию конституционного права гражданина на информацию и исключающее причинение вреда с помощью информации и информационных технологий здоровью и имуществу человека, его физическому, психическому и нравственному развитию [2].

1.2 Угрозы информационной безопасности

Главная цель информационной политики государства состоит в обеспечении информационной безопасности страны. Для ее достижения проводится спектр мероприятий, направленных на «формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации» [8].

Правовую основу информационной политики России в сфере безопасности составляют Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [55], а также Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646 [44]). Эти документы служат также основой для выработки мер, направленных на совершенствование системы информационной безопасности.

Основные информационные угрозы безопасности перечислены в разделе III Доктрины информационной безопасности Российской Федерации. В частности, в этом стратегическом документе указывается, что «в условиях глобальной информатизации население страны может подвергаться информационно-психологическому воздействию, направленному на разжигание межнациональной розни, дестабилизацию внутриполитической и социальной ситуации, подрыв суверенитета и нарушение территориальной целостности государства» [8]. Также «возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина» [18], и др.

Информационная угроза представляет собой определенное воздействие лицом или группой лиц на информационную систему для нанесения ущерба гражданам, обществу и государству.

Одной из серьезных информационных угроз является несанкционированный доступ к информационным ресурсам в сети Интернет, когда злоумышленник, незаконно получая размещенные там сведения, распространяет их, удаляет либо видоизменяет их контекст. В этой ситуации представляется необходимым детально контролировать, куда и по каким информационным каналам передается информация для недопустимости утечки передаваемых сведений. Если сведения передаются по незащищенным информационным каналам, следовательно, они могут попасть к злоумышленнику, который впоследствии может причинить вред владельцу информации.

Остановимся на информационных угрозах, причиняющих ущерб гражданам. Например, при хранении персональных сведений в мобильном электронном устройстве может возникнуть угроза доступа к ним с помощью специальных приложений и вредоносных программ. В результате могут быть совершены мошеннические действия посредством получения сведений о данных банковской карты владельца, что может привести к хищению денежных средств.

Чаще всего несанкционированный доступ к информационным сведениям граждан происходит путем кибератак, представляющих собой вредоносную попытку злоумышленника незаконно проникнуть в информационную систему гражданина, организации, государства. Кибератаки, исходя из способа воздействия, могут осуществляться с помощью:

- вредоносного программного обеспечения, т.е. вирусных программ, которые заражают электронные устройства или существенно замедляют их работу, а также собирают, копируют, передают или уничтожают информационные сведения;

– социальной инженерии, способствующей проведению манипуляционных действий с гражданами для совершения ими нужных для злоумышленника действий. В эту категорию следует отнести фишинг, представляющий собой рассылку электронных писем и сообщений, содержащих вредоносный код;
– «хакинга», т.е. незаконного действия злоумышленника, нацеленного на взлом определенных объектов информационной безопасности;
– подбора учетных сведений физических лиц (логинов и паролей в различных информационных системах) [39].

По статистическим данным, в 2023 году наиболее распространенными и опасными информационными угрозами были следующие: использование вредоносного программного обеспечения для организаций – 57%, для граждан – 63%; социальная инженерия для организаций – 37%, для граждан – 90%; эксплуатация уязвимостей для организаций – 35%, для граждан – 6%; компрометация учетных данных для организаций – 7%, для граждан – 1%; компрометация цепочки поставок или доверенных каналов связи для организаций – 7%, для граждан – 1%; другие угрозы для организаций – 13%, для граждан – 3%. При этом доля атакуемых объектов (компьютеры, серверы и сетевое оборудование) организаций составила 90%, граждан – 54%; сотрудников организаций – 37%, граждан – 90%; веб-ресурсы организаций – 27%, граждан – 3%; мобильные устройства граждан – 15%; другие угрозы для организаций – 4%, для граждан – 2% [1].

Несущественными можно считать угрозы информационной безопасности при выполнении трех условий:

– ресурсы каждого системного уровня обладают регламентированным уровнем защиты, позволяющим блокировать доступ несанкционированным попыткам считывания защищаемой информации;
– пользователи, обладающие доступом к определенному уровню информации, вправе вносить только те коррективы, которые

вытекают из их функционала. Не могут быть внесены в базу несанкционированные коррективы от имени каждого пользователя. Таким образом, осуществляется запрет на ее модификацию;

– следующим критерием минимизации угрозы безопасности является сокращение времени, необходимого для поиска требующейся информации.

Угрозы безопасности информации – это нарушение одного из трех вышеперечисленных принципов работы с массивами информации. Каждый из них имеет свои особенности практического применения. Первые два пункта наиболее уязвимы (подвержены воздействию злоумышленников). Защита от несанкционированного доступа обычно связана с угрозами извне (не со стороны пользователей информационной системы).

Защита от корректировок (модификаций информации) в первую очередь призвана обезопасить от действий пользователей информационной системы, которые могут неосознанно повредить ее.

Наконец, третий момент – это риск перегрузки базы данных. Эта угроза может исходить как от внутренних пользователей, так и от внешних источников, которые искусственно увеличивают трафик запросов на получение информации, после чего информационная система начинает работать некорректно [13].

Если говорить об информационных угрозах, причиняющих крупный ущерб государству, следует привести примеры кибервойн и кибертерроризма. С возникновением и дальнейшим развитием информационных технологий у многих государств появляются возможности проведения цифровых атак на информационные ресурсы недружественных стран, которые наносят ущерб и компьютерной системе государства, и безопасности страны. Такие явления именуются кибервойнами. Кража конфиденциальных сведений другой страны, их незаконное раскрытие и распространение – это общественно опасные действия, именуемые кибертерроризмом [60].

Констатируется, что кибервойны могут вестись не только странами, но и организациями, и даже отдельными государственными политиками. Следовательно, в такой войне оружием будут выступать средства массовой информации. Из-за большого числа информации, поступающей к гражданам, бывает сложно ориентироваться в ней, а значит, и ограждать себя от нежелательного потока сведений. Навязывание другой культуры, столкновение с виртуальной и фактической реальностью также выступают информационной и психологической угрозой для граждан.

Следует выделить три вида глобальных информационных угроз, которые могут причинить существенный вред государству:

- применение искусственного интеллекта в ходе установления предполагаемых жертв, уязвимостей программ, осуществления кибератак. При использовании возможностей искусственного интеллекта кибератаки становятся глобальными и наиболее изощренными, с причинением более серьезного ущерба. В современный период искусственный интеллект применяется в ходе создания реальных изображений и звуков. Применение таких инновационных технологий может, например, способствовать получению автомобилям-беспилотниками изображений людей-пешеходов, автомобилей в разнообразной обстановке без выезда при этом на проезжую часть. Применение синтезатора речи определенного человека может повлечь ситуацию, когда пользователь перейдет по ссылке, имеющей компьютерный вирус, или закачает необходимое для преступника электронное приложение;
- применение искусственного интеллекта в политике способствует возникновению манипуляций общественным мнением. При помощи искусственного интеллекта можно создать фейковую информацию в больших количествах, в результате чего пользователю информации довольно сложно отличить достоверные сведения от ложных

данных. В результате предоставления недостоверных сведений повышается адресность пропаганды. С применением возможностей искусственного интеллекта злоумышленники изучают поведенческие основы человека, которые впоследствии могут быть использованы в ходе манипуляций массовым сознанием;

– осуществление кибератак на различные объекты. Данные атаки могут быть применены в ходе массового использования беспилотников или других автоматизированных боевых комплексов. Могут возникнуть возможности незаконного внедрения в системы беспилотных автомобилей вредоносных программ для последующего проведения аварий и различных нападений.

Итак, в завершении главы исследования, необходимо сделать ряд важных выводов.

Во-первых, термин «информационная безопасность» применяется для обозначения двух различных понятий. Информационная безопасность в первом случае рассматривается в качестве практики предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это понятие обладает универсальностью – применяется независимо от формы, которую могут принимать сведения (электронная/физическая). Основной задачей обеспечения информационной безопасности с этой позиции является сбалансированная защита конфиденциальности, целостности и доступности информации. Тем самым, речь идет о защите данных, о мерах, принимаемых организацией для защиты различных типов информации. Важность этого направления деятельности определяется растущим числом угроз, связанных с цифровизацией различных сфер жизни общества, широким использованием информационных технологий и т.д.

Кроме того, термин «информационная безопасность» используется при изучении проблем безопасности личности.

Информационное общество – это социологическая и футурологическая концепция, которая рассматривает производство и использование научной, технической и другой информации как неотъемлемую часть общественного развития. Концепция информационного общества – это своего рода разновидность теории постиндустриального общества.

Во-вторых, информационная угроза представляет собой определенное воздействие лицом или группой лиц на информационную систему для нанесения ущерба гражданам, обществу и государству. Для граждан и организаций наиболее существенный ущерб причиняют несанкционированный доступ и кража данных, использование вредоносного программного обеспечения, социальная инженерия. Если говорить об информационных угрозах, причиняющих крупный ущерб государству, следует назвать кибервойны и кибертерроризм.

В-третьих, рост информационных угроз кибербезопасности влечет необходимость поиска механизмов противодействия применению информационных технологий в преступных действиях. Как представляется, основными мерами противодействия современным информационным угрозами должны выступать:

- развитие и дальнейшее функционирование системы постоянного мониторинга информационных систем для обеспечения национальной безопасности государства;
- выработка органами государственной власти и дальнейшее принятие государственных решений по предупреждению информационных угроз объектам безопасности;
- создание моделей устойчивого социального развития информационной системы в различных ситуациях.

Глава 2 Механизм обеспечения информационной безопасности

2.1 Правовой механизм обеспечения информационной безопасности

Исторически в России к защищаемой информации относились сведения из области государственной и военной тайны, предпринимались меры к охране коммерческой тайны. Методы и средства защиты информации каждой исторической эпохи были тесно связаны с уровнем развития науки, техники и технологий. Категории защищаемой информации определялись экономическими, политическими и военными интересами государства. Чаще всего защищалась информация, касающаяся:

- организации управления государством;
- обороны государства, военного дела;
- международных отношений;
- разведывательной деятельности. Деятельность по защите информации была обусловлена эволюцией политической и экономической структуры российского государства.

В современной России предметная область законодательства в сфере обеспечения информационной безопасности включает три подгруппы объектов защиты. К ним относятся:

- защита информации и прав на нее (включая право на доступ к информации, право на тайну, права на объекты интеллектуальной собственности);
- защита человека и общества от воздействия «вредной» информации;
- защита информационных систем и прав на них (в том числе прав и интересов государства по сохранению единого информационного пространства в стране).

Итак, в России законодательство в области обеспечения информационной безопасности начинает формироваться в начале 90-х годов прошлого столетия с закрепления основных прав и обязанностей, можно

сказать, что в этот период складывается правовая защита информации. Речь идет о закреплении на конституционном уровне:

- права на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23 Конституции РФ);
- запрета на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия (ст. 24 Конституции РФ);
- права свободного поиска, получения, передачи, производства и распространения информации любым законным способом (перечень сведений, составляющих государственную тайну, определяется федеральным законом) (ст. 29 Конституции РФ);
- права на достоверную информацию о состоянии окружающей среды (ст. 42 Конституции РФ) [19].

К этому же этапу можно отнести первые редакции Федерального закона от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации», который, устанавливал лишь базовые понятия в этой сфере. В частности, он определил функции государства в области защиты данных, создал пока только понятие об информационных ресурсах государства, включил их в общероссийское национальное достояние и т.д.

Правовой режим государственной тайны был установлен первым в истории российского государства Законом «О государственной тайне», который вступил в действие 21 сентября 1993 года (новая редакция Закона Российской Федерации «О государственной тайне» была принята в 1997 году) [12].

Президентским указом от 6 марта 1997 года № 188 был закреплен перечень сведений конфиденциального характера, таких как персональные данные, тайна судопроизводства, коммерческая тайна и т.д. [45].

Доктрина информационной безопасности Российской Федерации 2000 года (утверждена Президентом РФ 9 сентября 2000 г. № Пр-1895) ставила

перед собой основную задачу по защите личности в информационной сфере [7]. При этом интересы личности в информационной сфере заключаются не только в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития. В документе отмечается необходимость защиты информации, обеспечивающей личную безопасность.

В это время в России создается институт персональных данных, направленный на более эффективное обеспечение конфиденциальности и защиты персональных данных.

В Стратегии развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. № Пр-212) один из принципов, на которых базируется развитие информационного общества в России, – это обеспечение национальной безопасности в информационной сфере [38]. В качестве одного из направлений реализации Стратегией было названо обеспечение неприкосновенности частной жизни, личной и семейной тайны, соблюдение требований к обеспечению безопасности информации ограниченного доступа, что и подтвердила Доктрина 2016 года.

Разработка новой Доктрины была продиктована изменившимися реалиями, связанными с угрозами информационной безопасности, изменением в стратегическом планировании в сфере обеспечения национальной безопасности.

Для разрешения вопроса противодействия компьютерным атакам в 2017 г. был представлен, а впоследствии принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной структуры Российской Федерации» [54].

Можно сделать вывод, что этот этап формирует два основных направления: внутреннее (2000 год) и внешнее (2016 год). Именно в этих двух направлениях законодательство в области информационной безопасности формирует тандем состояния безопасности каждого человека,

общества и государства. На деле – направление развития права в сфере информационной безопасности создало возможность следовать тенденциям глобальной информатизации.

Таким образом, 90-е годы XX века, если рассматривать этот исторический период сквозь призму информатизации, информационной безопасности и права, нельзя оценивать в негативном ключе (по сравнению, например, с экономической, социальной и политической сферами). В формирующейся сфере информационной безопасности действия государства были прогрессивными и позитивными. Во всем мире, включая Россию, в 80-х и 90-х годах прошлого века шел масштабный процесс внедрения цифровых технологий в практические сферы деятельности общества, включая промышленность, науку, военное дело и финансовый сектор.

Так совпало, что в это время в России произошел сдвиг в парадигме государственного регулирования: произошел переход от административных методов управления экономикой к правовым методам, основанным на верховенстве закона. Концепция рыночного саморегулирования стала доминирующей в экономике. В то же время не были выбраны лучшие модели управления, а прошлый опыт оказался невостребованным и не учитывался. В результате были утрачены целые отрасли промышленности, такие как станкостроение и электроника, а система стандартизации была разрушена. Государственные стандарты утратили статус законодательного акта, что, несомненно, стало значительным шагом назад.

Вопросы информационной безопасности (тогда аппаратной защиты информации) были чисто прикладными, закрытыми по своей природе и недоступными для многих экспертов. Но работа была проделана, и она была адекватной современным реалиям. Приоритет был отдан вопросам, связанным с защитой информации от несанкционированного доступа, утечки сведений по радиотехническим каналам. Однако проблема защиты от несанкционированного доступа не была решена должным образом. Что касается моделирования угроз, то этот подход находился в зачаточном

состоянии, и внутренний класс нарушителей практически не рассматривался, впрочем, как и за рубежом.

Именно в этот период появилось само понятие «информационная безопасность», которому разные эксперты придавали разное значение:

- технические эксперты полагали, что это понятие теснейшим образом связано с понятием «защиты информации» и определяли его как «деятельность», а не как «состояние»;
- другая группа экспертов полагала, что информационная безопасность более широкое понятие, фокусирующееся на социально-политических и психологических аспектах существования и развития общества и государства. На самом деле различия в позициях исследователей сохраняется и сейчас, несмотря на то что в последнее время технические эксперты все чаще используют концепцию «кибербезопасности», которая ограничивает сферу рассмотрения и более точно отражает природу явления защиты информации.

В конце XX века система информационной безопасности, созданная в России по отраслевому принципу, постепенно начала разрушаться вместе с отраслями промышленности, в основном из-за недостатка финансирования, что негативно сказалось на научно-методической базе. В результате в России начали применяться зарубежные стандарты, за которыми последовал импорт продуктов и решений в основном в области информационных технологий, а затем и в области безопасности. На самом деле сильнейшая зависимость от импорта до сих пор не преодолена.

В начале 90-х годов прошлого века не существовало законодательства в области информатизации и информационной безопасности. Однако текущая ситуация потребовала оперативного создания фундаментальных нормативных актов в области информационной безопасности. В результате стало возможным разработать политическую стратегию, определить и в

целом реализовать приоритеты, которые задают долгосрочные ориентиры для развития вопросов информационной безопасности.

К ним относятся:

- создание государственной системы защиты данных, разработка законодательства в следующих областях: информатизация, информационная безопасность и защита информации; административное и уголовное законодательство, определяющее ответственность за компьютерные преступления; персональные данные; использование электронных цифровых подписей;
- разработка необходимой нормативно-правовой базы для технической защиты и последующий доступ к системе стандартизации;
- развитие государственной системы лицензирования, сертификации и аттестации;
- создание системы подготовки кадров в области информационной безопасности.

Следует выделить три вида глобальных информационных угроз, которые могут причинить существенный вред государству:

- применение искусственного интеллекта в ходе установления предполагаемых жертв, уязвимостей программ, осуществления кибератак. При использовании возможностей искусственного интеллекта кибератаки становятся глобальными и наиболее изощренными, с причинением более серьезного ущерба. В современный период искусственный интеллект применяется в ходе создания реальных изображений и звуков. Применение таких инновационных технологий может, например, способствовать получению автомобилям-беспилотниками изображений людей-пешеходов, автомобилей в разнообразной обстановке без выезда при этом на проезжую часть. Применение синтезатора речи определенного человека может повлечь ситуацию, когда

пользователь перейдет по ссылке, имеющей компьютерный вирус, или закачает необходимое для преступника электронное приложение;

- применение искусственного интеллекта в политике способствует возникновению манипуляций общественным мнением. При помощи искусственного интеллекта можно создать фейковую информацию в больших количествах, в результате чего пользователю информации довольно сложно отличить достоверные сведения от ложных данных. В результате предоставления недостоверных сведений повышается адресность пропаганды. С применением возможностей искусственного интеллекта злоумышленники изучают поведенческие основы человека, которые впоследствии могут быть использованы в ходе манипуляций массовым сознанием;
- осуществление кибератак на различные объекты. Данные атаки могут быть применены в ходе массового использования беспилотников или других автоматизированных боевых комплексов. Могут возникнуть возможности незаконного внедрения в системы беспилотных автомобилей вредоносных программ для последующего проведения аварий и различных нападений.

При создании государственной системы защиты данных приоритеты были смещены в сторону обеспечения государственных интересов. Смена приоритетов привела к необходимости создания эффективных отраслевых систем безопасности (Центральный банк Российской Федерации), ориентированных на другие модели угроз и решение практических задач в финансовом секторе. Одновременно началось перераспределение полномочий в системе государственного управления, в результате чего количество регулирующих органов в рабочих зонах достигло пяти (вместе с Министерством юстиции, утверждающим проекты нормативных актов, – шести) без учета отраслевых систем безопасности (силовых ведомств).

В результате такого подхода управление в устоявшейся системе при слабой властной вертикали становится более сложным и запутанным, цикл управления (от возникновения проблемы до появления регулирования (нормативного правового акта)) растягивается на годы, что приводит к задержкам в удовлетворении реальных потребностей. С практической точки зрения, существует очень большой разрыв между законодательством и реальной практической безопасностью, который служит основой для злоупотреблений и неправомерных действий.

В России примерно с конца 90-х годов прошлого века и начала 2000-х годов текущего столетия была сформирована необходимая законодательная база, позднее законодательство интенсивно менялось, модернизировалось. Вместе с тем, нельзя считать этот процесс завершенным, так как еще не нашли своего практического решения многие вопросы в изучаемой сфере.

Уместно более детально рассмотреть ряд вопросов в сфере государственно-правового механизма обеспечения информационной безопасности. Речь идет о защищенном сегменте сети Интернет для органов государственной власти и институте персональных данных.

Законодательство в области Интернета лежит на стыке правового поля и политики, так как напрямую затрагивает интересы общества, права и свободы человека. Задача создания защищенного сегмента сети Интернет для органов государственной власти получила свое развитие в Указе Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» [50].

Данный документ, по сути, запустил процедуру перевода международного сегмента сети интернет для органов власти, подведомственного Федеральной службе охраны (далее по тексту – ФСО), в российский сегмент. Данному ведомству было поручено поддерживать, эксплуатировать и развивать государственный сегмент интернета, созданный за счет сетей шифрованной связи, которые позволяют защищать информацию от несанкционированного доступа. В документе для ряда

государственных структур установлена обязательность подключения к «основному» интернету и размещения в нем информации только через государственный сегмент. Это касается администрации главы государства, аппарата правительства, органов государственной власти федерального и регионального уровня и др.

1 ноября 2019 г. вступил в силу Федеральный закон от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации», который в средствах массовой информации получил также название «О суверенном Рунете» [51].

«Суверенный Рунет» представляет собой независимую инфраструктуру для бесперебойного функционирования интернета в России. Цель принятия закона состоит в защите российского сегмента сети Интернет от внешних угроз, в том числе – отключения от Всемирной паутины и кибератак.

Согласно правовым нормам, операторы связи должны устанавливать в своих сетях технические средства для противодействия угрозам (ТСПУ). ТСПУ является программно-аппаратным комплексом, позволяющим ограничить доступ к данным, распространение которых запрещено на территории государства. В случае возникновения угроз целостности, стабильности и безопасности Интернета Роскомнадзор может использовать это устройство для централизованного управления маршрутизацией трафика, фильтрации трафика и ограничения доступа пользователей Рунета к запрещенным в стране ресурсам. Кроме того, этот закон ограничил подключение сетей связи к точкам обмена трафиком (физическое местоположение, где сети различных организаций (крупных компаний, Интернет-провайдеров, хостинг-провайдеров и т.д.) находятся в контакте друг с другом). Закон обязывает, среди прочего, владельцев сетей связи, интернет-компании и других участников рынка участвовать в ежегодных специализированных учениях. В этом законодательном акте также признается необходимость создания национальной системы доменных имен,

которая копировала бы список доменных имен и номера автономных систем, делегированных пользователям в России. Предусмотрена ответственность за несоблюдение операторами связи положений закона, регулирующего суверенный интернет.

В целом, Закон о суверенном Рунете довольно спорный и сложный проект, который имеет как плюсы, так и минусы и реализуется в зоне высокого риска. С одной стороны, он может повысить безопасность и стабильность работы интернета в России в случае возможных внешних угроз. С другой стороны, он вполне способен усилить контроль и цензуру над информацией в сети, а также ухудшить качество связи для пользователей. Закон требует больших затрат на его реализацию и поддержку, а также вызывает много вопросов по его технической осуществимости и правовой обоснованности. Закон также может повлиять на развитие цифровой экономики и инноваций в России, а также на ее интеграцию в мировое информационное пространство. Можно предположить, что на разных этапах реализации проекта суверенного Рунета потребуются как дополнительные финансовые затраты, так и законодательные инициативы и разработка дополнительных инструментов регулирования.

Что касается персональных данных, то данный институт, как уже отмечалось, был создан Законом о персональных данных 2006 г. [56] Он явился следствием договоренностей, достигнутых на Четырнадцатом саммите Россия – ЕС (Гаага, 25 ноября 2004 г.). Правительству РФ было поручено внести в Государственную Думу на ратификацию Конвенцию Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [15].

С того момента законодательство о персональных данных регулярно совершенствуется. В сентябре 2022 года были внесены новые поправки в законодательство о персональных данных, в том числе усовершенствован порядок их трансграничной передачи. Трансграничной передачей Роскомнадзор признает ситуации, например, когда российский оператор

хранит персональные данные контрагентов в GoogleDocs или обрабатывает данные пользователей сайта в GoogleAnalitycs.

Новая редакция ст. 12 Федерального закона «О персональных данных» устанавливает, что в перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, включаются государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. В этот перечень входят также иностранные государства, не являющиеся сторонами названной Конвенции Совета Европы при условии соответствия положениям Конвенции действующих в соответствующем государстве норм права и применяемых мер по обеспечению конфиденциальности и безопасности персональных данных при их обработке.

Еще до начала трансграничной передачи персональных данных оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять трансграничную передачу персональных данных. Закон определяет перечень содержащихся в таком уведомлении сведений: правовое основание и цель трансграничной передачи и обработки персональных данных; категории и перечень передаваемых персональных данных; категории субъектов персональных данных, чьи данные передаются; перечень иностранных государств, на территории которых планируется трансграничная передача персональных данных и другие сведения.

Закон предусматривает, что по решению уполномоченного органа власти трансграничная передача персональных данных может быть запрещена или ограничена в исключительных случаях.

Решение о запрете или ограничении трансграничной передачи персональных данных может быть принято в определенных законом целях: защиты основ конституционного строя и безопасности государства; обеспечения обороны страны; защиты экономических и финансовых интересов Российской Федерации; обеспечения дипломатическими и

международно-правовыми средствами защиты прав, свобод и интересов граждан Российской Федерации, суверенитета, безопасности, территориальной целостности страны. Как видно, перечень оснований запрета или ограничения трансграничной передачи персональных данных является закрытым и не допускается его расширение.

Уполномоченным органом по защите прав субъектов персональных данных является федеральный орган исполнительной власти, осуществляющий самостоятельно функции по контролю и надзору за соответствием обработки персональных данных требованиям национального законодательства в области персональных данных. Речь идет о Роскомнадзоре.

Закон подробно регламентирует порядок взаимодействия оператора и Роскомнадзора в случае неправомерной передачи, предоставления или распространения персональных данных, в результате которых произошло нарушение прав субъектов персональных данных. В этом случае Закон установил сокращенные сроки реагирования оператора на указанные нарушения прав субъектов персональных данных.

Если произошла утечка, то есть неправомерная передача персональных данных, оператор обязан сообщить об этом в Роскомнадзор. Оператор, который обрабатывает персональные данные на компьютере, дополнительно обязан работать с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак. Через нее следует сообщать об инцидентах, из-за которых произошла утечка данных.

После внесения ряда изменений в законодательство о защите персональных данных, общий уровень защищенности персональных данных граждан повысился, что послужило важной гарантией обеспечения конституционного права на неприкосновенность частной жизни.

Гражданин может потребовать в любое время у оператора сведения:

– о факте, основаниях, сроке, целях обработки и передачи персональных данных;

– наименовании и месте нахождения оператора;
– составе данных, источнике их получения. Такое требование устанавливают пункты 2, 7 ст. 14 Закона о персональных данных.

Если будет обнаружено, что оператор обрабатывает персональные данные, хотя они неточные, гражданин может потребовать их обновить, заблокировать или совсем удалить. То же самое можно сделать, если оператор получил персональные данные незаконно или если они избыточны. Обработка и хранение лишних персональных данных – это распространенная ошибка операторов (п. 1 ст. 14 Закона о персональных данных).

Операторы вправе передавать данные компаниям, которые продвигают товары, работы, услуги или занимаются политической агитацией, только с согласия субъекта персональных данных. Дать такое согласие – это право гражданина, а не его обязанность. Поэтому без согласия оператор обязан перестать использовать данные (ст. 15 Закона о персональных данных).

Субъект персональных данных может потребовать у оператора разъяснить, как происходит такая обработка, и какие последствия она влечет. В любой момент субъект вправе предоставить возражение против автоматизированной обработки. Оператор рассмотрит его и даст ответ в течение 30 дней (ст. 16 Закона о персональных данных).

Субъект может возражать против обработки информации вычислительной техникой, так как она может быть неточной и не должна порождать юридические последствия. Например, пройти по электронному пропуску сотрудника может другой гражданин (п. 6 ч. 1 ст. 81 ТК РФ) [41].

Субъект может возражать и против неавтоматизированной обработки данных, если не хочет давать информацию о себе оператору. В большинстве случае после такого отказа оператор не станет оказывать услуги гражданину, чтобы не нарушить Закон о персональных данных.

Если есть основания полагать, что оператор персональных данных нарушил права субъекта, последний вправе обратиться в Роскомнадзор,

прокуратуру или суд. В иске заявляются требования о возмещении убытков и компенсации морального вреда (ст. 17 Закона о персональных данных).

По общему правилу субъект персональных данных вправе отозвать свое согласие на обработку персональных данных в любое время. Однако есть случаи, когда оператор вправе обрабатывать данные и после отзыва согласия. Чтобы отозвать согласие на обработку и распространение персональных данных, обращение направляется в адрес оператора в любой момент (ст. 9 Закона о персональных данных).

По общему правилу оператор обязан прекратить обработку и распространение персональных данных по требованию субъекта, отзывающего свое согласие на осуществление этих действий. Оператор обязан прекратить распространение в течение трех рабочих дней с момента получения отзыва. Чтобы прекратить другую обработку, у оператора будет 30 дней. По истечении этого срока он не имеет права использовать персональные данные для своих целей (п. 14 ст. 10.1, п. 5 ст. 21 Закона о персональных данных).

При этом в законе есть исключения. Оператор может продолжить обработку информации даже после отзыва, чтобы: 1) направить бухгалтерскую отчетность; 2) хранить кадровые документы; 3) исполнить другие обязанности работодателя. Такие правила устанавливают подпункты 2–11 пункта 1 статьи 6, пункт 2 статьи 10 и пункт 2 статьи 11 Закона о персональных данных. Иные действия по обработке данных оператор должен согласовать с субъектом персональных данных. Отзыв согласия на обработку персональных данных направляется непосредственно оператору.

Если оператором нарушены права гражданина в сфере персональных данных, их защиту осуществляет Роскомнадзор, прокуратура или суд. В Роскомнадзор и прокуратуру направляется жалоба в письменной форме с указанием:

- как оператор нарушил права субъекта персональных данных;
- положения закона, которые нарушил оператор;

– персональные данные, которые незаконно используют;
– сведения об операторе;
– требования.

В суд подается иск без соблюдения досудебного порядка урегулирования спора. По общему правилу иск подают по месту нахождения ответчика-оператора. Закон разрешил предъявлять требования в суд также и по месту нахождения истца (ст. 24, п. 6.1 ст. 29 ГПК РФ). В иске указываются:

– как оператор нарушил права субъекта персональных данных;
– положения закона, которые нарушил оператор;
– персональные данные, которые незаконно используют;
– сведения об операторе;
– требования заявителя;
– размер ущерба и компенсации морального вреда.

В целом, можно сказать, что сегодня законодательство о защите персональных данных развивается довольно интенсивными темпами, но информационные технологии, Интернет, различные мобильные приложения и т.д. развиваются еще более стремительно. Совершенно очевидно, что российскому законодателю и соответствующим государственным органам не всегда удается регулировать весь поток информации персонального характера с юридической точки зрения, поэтому одним из приоритетов современного российского общества является постоянный анализ и мониторинг развития информационных технологий.

2.2 Органы государственной власти и их деятельность в области обеспечения информационной безопасности

Компетенция федеральных органов государственной власти, органов государственной власти субъектов РФ, других государственных органов, входящих в состав системы обеспечения информационной безопасности

Российской Федерации и ее подсистем, определяется федеральными законами, нормативными правовыми актами Президента РФ и Правительства РФ.

Функции органов, координирующих деятельность федеральных органов государственной власти, органов государственной власти субъектов РФ и других государственных органов, входящих в состав системы обеспечения информационной безопасности Российской Федерации и ее подсистем, определяются отдельными нормативными правовыми актами РФ.

К числу таких органов, в частности, относятся Межведомственная комиссия Совета Безопасности РФ по информационной безопасности, Военно-промышленная комиссия РФ, Межведомственная комиссия по защите государственной тайны и др.

Система обеспечения информационной безопасности Российской Федерации является частью системы обеспечения национальной безопасности государства. Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются: Президент РФ, Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума, Правительство РФ, Совет Безопасности РФ, федеральные органы исполнительной власти, межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, органы исполнительной власти субъектов РФ, органы местного самоуправления, органы судебной власти, общественные объединения, граждане, принимающие в соответствии с законодательством РФ участие в решении задач по обеспечению информационной безопасности Российской Федерации.

Президент РФ руководит в пределах своих конституционных полномочий органами и силами по обеспечению информационной безопасности страны; санкционирует действия по обеспечению информационной безопасности государства; в соответствии с законодательством РФ формирует, реорганизует и упраздняет подчиненные

ему органы и силы по обеспечению информационной безопасности Российской Федерации; определяет в своих ежегодных посланиях Федеральному Собранию приоритетные направления государственной политики в области обеспечения информационной безопасности Российской Федерации, а также меры по реализации положений Доктрины информационной безопасности.

Палаты Федерального Собрания РФ на основе Конституции РФ по представлению Президента РФ и Правительства РФ формируют законодательную базу в области обеспечения информационной безопасности государства.

Правительство РФ в пределах своих полномочий и с учетом сформулированных в ежегодных посланиях Президента РФ Федеральному Собранию приоритетных направлений в области обеспечения информационной безопасности Российской Федерации координирует деятельность федеральных органов исполнительной власти и региональных органов исполнительной власти (в рамках установленной компетенции).При формировании в установленном порядке проектов федерального бюджета на соответствующие годы предусматривает выделение средств, необходимых для реализации федеральных программ в этой области.

Совет Безопасности РФ проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации, оперативно подготавливает проекты решений Президента РФ по предотвращению таких угроз. Совет Безопасности РФ разрабатывает предложения в области обеспечения информационной безопасности Российской Федерации, а также предложения по уточнению отдельных положений Доктрины, координирует деятельность органов и сил по обеспечению информационной безопасности Российской Федерации, контролирует реализацию федеральными органами исполнительной власти и органами исполнительной власти субъектов РФ решений Президента РФ в этой области.

Федеральные органы исполнительной власти обеспечивают исполнение законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности Российской Федерации; в пределах своей компетенции разрабатывают нормативные правовые акты в этой области и представляют их в установленном порядке Президенту РФ и в Правительство РФ.

Межведомственные и государственные комиссии, создаваемые Президентом РФ и Правительством РФ, решают в соответствии с предоставленными им полномочиями задачи по обеспечению информационной безопасности Российской Федерации.

Региональные органы исполнительной власти взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства РФ, решений Президента РФ и Правительства РФ в области обеспечения информационной безопасности Российской Федерации, а также по вопросам реализации федеральных программ в этой области. Совместно с органами местного самоуправления региональные органы исполнительной власти осуществляют мероприятия по привлечению граждан, организаций и общественных объединении к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Органы местного самоуправления обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности Российской Федерации.

Органы судебной власти осуществляют правосудие по делам о преступлениях, сказанных с посягательствами на законные интересы личности, общества и государства в информационной сфере, и обеспечивают судебную защиту граждан и общественных объединений, чьи права были

нарушены в связи с деятельностью по обеспечению информационной безопасности Российской Федерации.

В состав системы обеспечения информационной безопасности Российской Федерации могут входить подсистемы (системы), ориентированные на решение локальных задач в данной сфере.

К числу уполномоченных федеральных органов исполнительной власти в области обеспечения информационной безопасности относятся, прежде всего, ФСБ России, ФСТЭК России, ФСО России, Минцифры России, подведомственный ему Роскомнадзор.

В деятельности ФСБ России одним из основных направлений является «обеспечение информационной безопасности, осуществляемое при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств, а также при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях, находящихся за пределами страны, а также обеспечения безопасности автоматизированных систем управления критически важных объектов» [47].

ФСТЭК России является «федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля, а также органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну и органом, уполномоченным организовывать деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководства ею» [49].

ФСО России является «федеральным органом исполнительной власти в области государственной охраны, осуществляющим функции по выработке и реализации государственной политики, нормативно-правовому регулированию, контролю и надзору в сфере государственной охраны, связи для нужд органов государственной власти, а также функции по информационно-технологическому и информационно-аналитическому обеспечению деятельности Президента РФ, Правительства РФ, иных государственных органов» [46].

Минцифры России является «федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий (включая использование информационных технологий при формировании государственных информационных ресурсов и обеспечение доступа к ним), электросвязи (включая использование и конверсию радиочастотного спектра) и почтовой связи, массовых коммуникаций и СМИ, в том числе электронных (включая развитие сети Интернет, систем телевизионного (в том числе цифрового) вещания и радиовещания и новых технологий в этих областях), печати, издательской и полиграфической деятельности, обработки персональных данных» [28].

В ведении Минцифры России находится Роскомнадзор – федеральная служба, для которой функция по контролю (надзору) является основной. Роскомнадзор является «федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере СМИ, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства РФ в области персональных данных, а также функции по организации деятельности радиочастотной службы. Роскомнадзор является уполномоченным федеральным органом исполнительной власти по защите прав субъектов персональных данных» [29].

В заключение главы исследования необходимо сделать ряд важных выводов.

Во-первых, исторически в России к защищаемой информации относились сведения из области государственной и военной тайны, предпринимались меры к охране коммерческой тайны. Методы и средства защиты информации каждой исторической эпохи были тесно связаны с уровнем развития науки, техники и технологий. Категории защищаемой информации определялись экономическими, политическими и военными интересами государства. Российское законодательство отражает постепенное формирование правовой базы для регулирования отношений в данной сфере, однако стремительное развитие информационных и телекоммуникационных технологий, особенно Интернета, не позволяет своевременно обновлять, вносить изменения и дополнения в правовую базу.

Во-вторых, сама сфера рассматриваемых отношений сложна для регулирования в силу множества причин:

- современные средства защиты информации часто неадекватны текущим вызовам и угрозам информационной безопасности;
- многообразие и разнообразие способов совершения правонарушений, преступлений в сети Интернет;
- сложность выявления и отслеживания нарушений законодательства в сети Интернет.

В-третьих, организационное обеспечение информационной безопасности в стране конкретизирует способы и средства реализации потенциала правового обеспечения информационной безопасности.

В-четвертых, в настоящее время в России приняты документы, которые определяют стратегический подход государства к защите государственных интересов в целом, например, Доктрина информационной безопасности. Вектор развития законодательства в отдельных отраслях обозначен в соответствующих Стратегиях. Кроме того, принимаются многочисленные федеральные законы, которые часто не предвосхищают, а, наоборот,

являются реакцией на уже происходящие события (к моменту принятия законодательный акт в рассматриваемой сфере нередко утрачивает свою актуальность).

Регулирование отношений в сфере информационно-коммуникационных технологий должно в равной степени защищать интересы государства, бизнеса и граждан. Однако сегодня оно сводится в основном к введению запретов и ограничений, которые не только не способствуют технологическому развитию страны, но и серьезно его тормозят. В этой связи законодательному регулированию в изучаемой сфере необходим принципиально новый подход.

Органы местного самоуправления обеспечивают соблюдение законодательства РФ в области обеспечения информационной безопасности Российской Федерации.

Глава 3 Вопросы обеспечения информационной безопасности в отдельных сферах общественной жизни

3.1 Обеспечение информационной безопасности несовершеннолетних как составляющая национальной безопасности России

На глобальном уровне сегодня каждый третий пользователь сети Интернет моложе 18 лет [22]. Информационно-коммуникационные технологии предоставляют молодым людям бесчисленные возможности для общения, творчества, приобретения новых знаний и навыков, участия в жизни общества. Точно так же информационно-коммуникационные технологии могут создавать новые риски, связанные с вопросами конфиденциальности информации, незаконным контентом, кибербуллингом, неправомерным использованием персональных данных и т. д.

Сегодня в большом числе стран мира финансируют программы повышения цифровой грамотности и обеспечения безопасности детей в цифровой среде. Важными участниками разработки решений для обеспечения информационной безопасности несовершеннолетних являются родители (законные представители), образовательные учреждения, технологические компании и государственные учреждения. Идея активного обмена информацией пользуется широкой международной поддержкой, прилагаются совместные усилия по обеспечению безопасности детей в цифровой среде. Задача по-прежнему состоит в том, чтобы найти баланс между возможностями и рисками, связанными с деятельностью детей в цифровой среде. Хотя усилия по расширению возможностей детей по использованию информационно-коммуникационных технологий должны оставаться приоритетными, они должны быть сбалансированы с правами на безопасную информационную среду.

Опыт зарубежных стран показывает приоритет глобальных ценностей в реализации политики обеспечения информационных прав ребенка, а также следование предписаниям, сформулированным в нормативных правовых актах международного уровня с учетом текущих тенденций развития информационно-коммуникационных технологий. Ключевой документ международного уровня в этой сфере – Конвенция ООН «О правах ребенка». В документе закреплены четыре общих принципа, призванные содействовать толкованию всей совокупности положений Конвенции и, соответственно, определению правильных направлений при осуществлении национальных программ по их выполнению. Они излагаются, в частности, в статьях 2, 3, 6 и 12 Конвенции. Речь идет о:

- недискриминации (ст. 2);
- наилучшем обеспечении интересов ребенка (ст. 3);
- праве на жизнь, выживание и развитие (ст. 6);
- взглядах ребенка (ст. 12) [17].

На национальном уровне приняты отдельные нормативные правовые акты, касающиеся информационной безопасности несовершеннолетних, в которых конкретизируется понятие информационной безопасности в их отношении. Так, Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее по тексту – Закон о защите детей от информации), определяет виды информации, причиняющей вред здоровью и развитию детей [57].

К такой информации относят:

- информацию, запрещенную для распространения среди детей;
- информацию, распространение которой ограничено среди детей определенных возрастных категорий (ст. 5 Закона о защите детей от информации).

Рассматриваемый законодательный акт призван защитить психику детей от негативного воздействия деструктивного контента, нейтрализовать риски развития порочных наклонностей и противоправной активности. К

запрещенной информации отнесен контент, способный вызвать у несовершеннолетних страх, панику и ужас, оправдывающий применение насилия, аморальные и противоправные поступки.

В целях ограничения доступа к сайтам в сети Интернет, которые содержат информацию, распространение которой в РФ запрещено, создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено» [30]. Необходимость в создании такого реестра обусловлена «недопущением распространения детской порнографии через веб-сайты, рекламы для привлечения несовершеннолетних в качестве участников в мероприятиях порнографического характера, информации о методах самоубийства и пропаганды употребления наркотиков и алкоголя» [30].

Помимо вышеуказанных нормативных правовых актов, основу законодательства в области информационной безопасности детей составляют положения Федерального закона от 24 июля 1998 г. № 124 «Об основных гарантиях прав ребенка в Российской Федерации». Указанный нормативный правовой акт установил обязанность со стороны органов государственной власти, органов местного самоуправления, должностных лиц оказания ребенку содействия «в реализации и защите его прав и законных интересов с учетом возраста ребенка и в пределах установленного законодательством объема дееспособности ребенка посредством принятия соответствующих нормативных актов, проведения методической, информационной и иной работы с ребенком по разъяснению его прав и обязанностей, порядка защиты прав, установленных законодательством, а также посредством поощрения исполнения ребенком обязанностей поддержки практики правоприменения в области защиты его прав и законных интересов» [53].

Стоит отметить, что еще в «Национальной стратегии действий в интересах детей на 2012-2017 годы» одной из проблем было названо именно обеспечение информационной безопасности детей [43]. Разработчики данной стратегии предложили ряд мер, которые должны были гарантировать информационную безопасность с детства.

Распоряжением Правительства России от 29 мая 2015 г. № 996-р была утверждена Стратегия развития воспитания в Российской Федерации на период до 2025 года. В соответствии с этим документом было предложено расширить воспитательные возможности информационных ресурсов путем: «создания условий, методов и технологий для использования возможностей информационных ресурсов, в первую очередь информационно-телекоммуникационной сети «Интернет», в целях воспитания и социализации детей; информационного организационно-методического оснащения воспитательной деятельности в соответствии с современными требованиями; содействия популяризации в информационном пространстве традиционных российских культурных, в том числе эстетических, нравственных и семейных ценностей и норм поведения; воспитания в детях умения совершать правильный выбор в условиях возможного негативного воздействия информационных ресурсов; обеспечения условий защиты детей от информации, причиняющей вред их здоровью и психическому развитию» [32].

Распоряжением Правительства от 28 апреля 2023 г. № 1105-р была утверждена новая концепция информационной безопасности детей. Главная цель концепции – защитить детей от информационных угроз и рисков в современной цифровой среде [31]. Задачи государства согласно документу состоят в: «повышении уровня информационной безопасности и цифровой грамотности несовершеннолетних; увеличении устойчивого спроса на получение высококачественной информационной продукции; сокращении числа детей, пострадавших от жестокого обращения и травли, в том числе онлайн; снижении вовлеченности несовершеннолетних в деструктивные

онлайн-группы; сокращении количества информации, причиняющей вред здоровью и (или) развитию детей; увеличении цифрового контента, направленного на формирование у детей традиционных ценностей»[31].

Необходимо учитывать все существующие угрозы в их комплексе:

- угрозы технологического характера, связанные с распространением вредоносного программного обеспечения, риском несанкционированного доступа к информации;
- угрозы, связанные с вредным или оскорбительным контентом, с которым сталкивается пользователь в Интернете;
- угрозы домогательств в отношении несовершеннолетних, включая любую форму нежелательного контакта, внимания, издевательств, насилия, связанных с общением в Интернете;
- угрозы, связанные с раскрытием личной или конфиденциальной информации, персональных сведений;
- угрозы, определяющие возникновение рисков социализации и негативных изменений в развитии личности детей и подростков, наносящие ущерб их физическому и (или) психическому здоровью информацией независимо от источника ее получения.

Тем самым можно выделить следующие группы рисков информационной безопасности несовершеннолетних: контентные риски; коммуникационные риски; технические риски; потребительские риски; интернет-зависимость [37].

В соответствии с указанными выше группами угроз должны быть определены наиболее важные меры по обеспечению информационной безопасности детей. В соответствии с принятыми научными подходами определяются основные направления обеспечения информационной безопасности несовершеннолетних. Так, в частности, на дошкольном и младшем школьном уровне это меры по защите детей от негативного воздействия информации (ограждающий подход), меры по формированию информационной культуры, культуры безопасного поведения в сети

Интернет. На уровне школьного образования все большее значение приобретают обучающий, образовательный и личностно-развивающий подходы, предполагающие формирование информационной культуры детей и подростков.

3.2 Система правового обеспечения международной информационной безопасности в условиях геополитических трансформаций

Право является ключом к обеспечению информационной безопасности на глобальном уровне. Правовая регламентация отношений в сфере обеспечения международной информационной безопасности обладает междисциплинарным характером. Она включает «систему теоретических и методологических правовых вопросов по применению государствами стандартов, правил и принципов ответственного поведения в цифровой среде. Эти правила призваны содействовать формированию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды» [27, с. 138].

Среди национальных интересов в сфере применения информационно-коммуникационных технологий одним из наиболее значимых является защита государственного суверенитета в цифровом пространстве [4, с. 26]. Значимое место в системе правовой регламентации рассматриваемых отношений принадлежит нормам международного информационного права.

В Основах государственной политики Российской Федерации в области международной информационной безопасности (далее по тексту – Основы) 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»(п. 6) [48].

Международная информационная безопасность – это понятие, которое было предложено и активно продвигается Россией на уровне мирового сообщества. Оно охватывает не только технические аспекты безопасности, но и политические и идеологические угрозы. Этот подход отличается от западной концепции кибербезопасности, которая сконцентрирована на технологической составляющей информационных угроз.

Международная информационная безопасность предполагает, что угрозы могут проистекать не только из технических недостатков и уязвимостей, но и из политических и идеологических факторов. Концепция международной информационной безопасности, предложенная Россией, подчеркивает, что влияние информации на политические и социальные процессы может быть опасным и требует адекватного реагирования. Однако западная концепция кибербезопасности в основном сосредоточена на технической стороне вопроса – защите компьютерных систем от хакеров, вирусов и других технических угроз.

Такое различие в подходах к информационной безопасности между Россией и западными странами вызывает напряженность в международных отношениях. Необходимость разрешения этого противоречия и достижение консенсуса на глобальном уровне остается актуальной задачей для международного сообщества, что требует конструктивного диалога и взаимопонимания между различными государствами и акторами в сфере обеспечения международной информационной безопасности [20, с. 6].

Основы в качестве цели государственной политики страны в области международной информационной безопасности называют «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»(п. 9).

Достижение данной цели осуществляется путем решения задач по развитию международного сотрудничества России на глобальном, региональном, многостороннем и двустороннем уровнях по вопросам формирования системы обеспечения международной информационной безопасности, а также противодействия ее основным угрозам (п. 10).

Стратегические задачи российской государственной политики в рассматриваемой области включают в себя:

- продвижение на международной арене российских подходов к развитию системы обеспечения международной информационной безопасности и российских инициатив в данной области;
- содействие формированию международно-правовых механизмов предотвращения (урегулирования) конфликтов государств в глобальном информационном пространстве;
- организацию межведомственного взаимодействия при реализации государственной политики в области международной информационной безопасности (п. 5 Основ).

В контексте осуществления названных стратегических задач Основы закрепили ключевые ориентиры реализации национальной политики в изучаемой сфере. Их важный элемент – системное совершенствование правового обеспечения международной информационной безопасности.

В числе названных ориентиров безусловный приоритет отдан координации усилий международного сообщества по принятию государствами-членами ООН Конвенции об обеспечении международной информационной безопасности. Российской Федерацией еще в 2011 г. была представлена концепция Конвенции об обеспечении международной информационной безопасности. В 2021 г. была подготовлена ее обновленная редакция. Этот документ должен был стать основой для создания международного правового инструмента, направленного на защиту информационных систем от кибератак и других угроз. Конвенция предполагала установление единого международного механизма

сотрудничества и координации в области кибербезопасности, а также разработку общих международных стандартов и принципов в этой сфере. Однако реализация данной концепции столкнулась с рядом трудностей и препятствий, и до сих пор не удалось добиться широкого согласия со стороны международного сообщества (в основном из-за позиции США и западных стран). Несмотря на это, проблема кибербезопасности остается одной из ключевых в современном мире, и требует совместных усилий государств для ее эффективного решения.

Отсутствие единого и всеобъемлющего международного договора в сфере международной информационной безопасности не свидетельствует о том, что в настоящее время эта сфера отношений лишена регулирования. Напротив, существует ряд международных нормативных правовых актов, резолюций и рекомендаций, которые касаются защиты информации и кибербезопасности. Они включают в себя документы ООН, международных организаций и нормы международного права, которые регулируют поведение государств в киберпространстве. Поэтому, хотя и отсутствует универсальный документ, который бы охватывал все аспекты международной информационной безопасности, существующие международные нормы и стандарты играют важную роль в обеспечении безопасности в цифровом пространстве.

Во-первых, начиная с 1998 г., Генеральной Ассамблеей ООН был принят ряд резолюций под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» [9]. Эти документы отражают важность обеспечения безопасности в сфере применения информационно-коммуникационных технологий на глобальном уровне. Принятие подобных документов свидетельствует о растущем осознании мировым сообществом необходимости адаптации международных правил и стандартов к стремительно развивающимся информационно-коммуникационным технологиям. Тем самым, прогресс в области информационных технологий требует системного подхода к обеспечению

информационной безопасности, как на национальном, так и на международном уровне.

В контексте международной безопасности процессы информатизации представляют собой двусторонний вызов: с одной стороны, они открывают новые возможности для сотрудничества и развития, с другой – ставят перед мировым сообществом новые вопросы в области обеспечения кибербезопасности (технологии и средства потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международной стабильности и безопасности). Документы, принятые Генеральной Ассамблеей ООН, призывают к сотрудничеству между государствами, международными организациями и частным сектором с целью разработки международных стандартов и норм, направленных на обеспечение безопасности информационных систем и данных.

Одним из ключевых аспектов в этих документах является признание права каждого государства на защиту своих информационных ресурсов и киберпространства, а также призыв к сотрудничеству и обмену информацией в случае кибератак и других угроз информационной безопасности.

Таким образом, ряд резолюций под названием «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» играют важную роль в формировании международного правового поля, направленного на обеспечение безопасности в цифровую эпоху. Однако указанные резолюции не носят юридически обязывающего характера.

Во-вторых, «в 2000-е гг. был принят ряд международных документов политического характера по вопросам развития информационного общества, в которых значительное внимание было уделено вопросам безопасности использования информационно-коммуникационных технологий» [11], [26], [42].

В-третьих, «борьба с определенными угрозами международной информационной безопасности частично регулируется универсальными и региональными международными соглашениями в области средств массовой информации и Интернета, а также в области борьбы с преступностью и терроризмом» [6], [16], [59].

В-четвертых, в рамках ООН были приняты добровольные и необязательные стандарты ответственного поведения государств в области применения информационно-коммуникационных технологий.

В-пятых, «на региональном и двустороннем уровнях был принят ряд обязательных международных соглашений в области международной информационной безопасности» [35], [36].

Также, стоит отметить, что не так давно были намечены перспективы принятия международного соглашения в области борьбы с преступлениями в сфере информационно-коммуникационных технологий [25].

Россия инициировала учреждение специального профильного комитета ООН для подготовки международного договора в этой сфере отношений. В 2021 году Россия представила в этот комитет проект Конвенции ООН о борьбе с использованием информационно-коммуникационных технологий в преступных целях. Кроме того, проект Конвенции также направлен на защиту прав человека и основных свобод в сфере информационных технологий. Россия призывает все страны присоединиться к этому проекту и совместно работать над созданием эффективного международного механизма борьбы с киберпреступностью. Без сомнения это важный шаг в обеспечении безопасности и стабильности в сфере использования информационных технологий и защите прав и свобод всех людей.

Текущее состояние отношений России и стран Запада характеризуется непреодолимыми противоречиями, откровенно враждебной, агрессивной позицией западных стран по отношению к России. В этих обстоятельствах фокус внимания России смещается на разработку соглашений в рамках

региональных международных организаций, участницей которых она является, и достижение договоренностей на двусторонней основе.

Помимо региональных объединений Евразийского экономического союза (ЕАЭС), БРИКС и Шанхайской организации сотрудничества (ШОС), существуют и другие важные форматы, играющие значимую роль в аспекте сотрудничества в области обеспечения международной информационной безопасности. Среди них следует отметить Содружество Независимых Государств (СНГ), Организацию Договора о Коллективной Безопасности (ОДКБ) и Союзное государство России и Республики Беларусь.

Опыт сотрудничества в этих форматах демонстрирует приверженность общим идеям достижения стабильности и процветания в регионе. Вопросам обеспечения международной информационной безопасности также уделяется повышенное внимание. Так за два десятилетия усилиями этих объединений были разработаны и приняты важные документы в изучаемой сфере, которые направлены на укрепление сотрудничества и защиту интересов государств-участников в сфере информационной безопасности.

Среди них можно выделить международные договоры, которые регулируют вопросы защиты информации, борьбы с киберпреступностью и обмена информацией между государствами. Такие документы являются важным инструментом для обеспечения стабильности и безопасности в регионе.Важно отметить, что сотрудничество в области международной информационной безопасности является неотъемлемой частью общего процесса укрепления международной безопасности и стабильности. Именно поэтому региональные объединения и форматы, такие как ЕАЭС, БРИКС, ШОС, СНГ, ОДКБ и Союзное государство России и Республики Беларусь, продолжают активно развивать свое сотрудничество в этой области.

Например, повестка цифрового сотрудничества является одной из самых важных и востребованных в странах БРИКС. К 2015 году этот вопрос обрел статус самостоятельного благодаря усилиям России, поскольку российские инициативы в области международной информационной

безопасности не ограничиваются сотрудничеством в рамках БРИКС и уже много лет поддерживаются на уровне ООН.

В 2015 году в Москве состоялась первая встреча министров связи стран БРИКС, на которой впервые были объявлены приоритеты многостороннего сотрудничества в области информационно-коммуникационных технологий. В список приоритетов вошли экономические вопросы, диверсификация мирового рынка программного обеспечения и информационно-технологического оборудования, а также проблемы политического взаимодействия, главным образом сотрудничества в области международной информационной безопасности.

На протяжении последних лет повестка цифрового сотрудничества стран БРИКС освещалась в контексте вопросов, связанных с инфраструктурным сотрудничеством и цифровой безопасностью. Первое направление, характеризующееся приоритетным значением развития цифровой инфраструктуры и передовых отраслей (связь, облачные вычисления, искусственный интеллект и т.п.), было закреплено под влиянием Китая, который выступил с рядом инициатив в этой области, что связано с желанием укрепить позиции Китая как ведущего центра силы в цифровом пространстве. Китай в 2022 году поставил перед собой цель сформировать сообщество с общей судьбой в киберпространстве, которое требует уважения цифрового суверенитета и обеспечения безопасности данных как ключа к успешному развитию цифровых инициатив.

В сфере обеспечения международной информационной безопасности можно выделить два направления сотрудничества – координация внешней политики государств для продвижения этой повестки в ООН (сюда входят вопросы, связанные с обеспечением цифрового суверенитета) и институционализация совместных усилий государств, прежде всего в рамках антитеррористической повестки БРИКС. Таким образом, обеспечение государственного суверенитета в информационно-коммуникационной среде является частью более широкой цифровой повестки в рамках БРИКС с

акцентом на вопросы обеспечения международной информационной безопасности.

В целом, участие в таких региональных организациях и подписание международных договоров в области международной информационной безопасности позволяет государствам-участникам эффективно справляться с современными угрозами и вызовами в сфере использования информационно-коммуникационных технологий. Это также способствует укреплению доверия между государствами и созданию благоприятной обстановки для развития экономики и социальной сферы в регионе [58, с. 62].

Поскольку регулирование международной информационной безопасности на глобальном уровне традиционными правовыми источниками пока недостаточно развито, следовательно, большое значение приобретают акты «мягкого права». На данный момент разработан и применяется свод международных правил, норм и принципов ответственного поведения государств в информационном пространстве. Смысл этих правил состоит в формировании правовой основы мирного взаимодействия государств в цифровом пространстве, обеспечить предотвращение войн, конфронтации и любых агрессивных действий.

В завершении главы исследования подведем итоги.

Во-первых, развитие информационно-коммуникационных технологий ставит перед государством задачу создания для несовершеннолетних лиц, как наиболее уязвимой категории населения (в силу возраста, психической незрелости и отсутствия жизненного опыта), безопасной информационной среды. Стратегическая цель государства состоит в создании условий для гармоничного развития подрастающего поколения, нейтрализации рисков и угроз, обусловленных стремительным развитием информационно-коммуникационных технологий. Обеспечение безопасной информационной среды для детей требует совместных усилий родительской общественности, образовательных организаций, государственных структур и технологических компаний. Осведомленность, информационная культура и технологические

инструменты в комплексе играют ключевую роль в защите детей от информационных угроз.

Можно выделить следующие группы рисков информационной безопасности несовершеннолетних: контентные риски; коммуникационные риски; технические риски; потребительские риски; интернет-зависимость.

Во-вторых, текущее правовое регулирование обеспечения информационной безопасности несовершеннолетних в России довольно разнообразно. На федеральном уровне приняты законодательные акты, определившие основные понятие в изучаемой сфере, субъектный состав и содержание отношений по обеспечению информационной безопасности детей, меры ответственности за нарушение законодательных требований и т.д. Региональные органы власти, в рамках предоставленных им полномочий, самостоятельно определяют мероприятия по обеспечению информационной безопасности детей, опираясь на положения Концепции информационной безопасности детей. Регулирование отношений в этой сфере на уровне регионов обладает определенной спецификой. Региональные нормативные правовые акты могут устанавливать собственные критерии определения деструктивного контента и содержать правовые механизмы его ограничения и др.

В-третьих, сегодня важность и значимость подготовки нормативных оснований регулирования информационной сферы и обеспечения ее безопасного развития признается практически всеми государствами. В настоящее время наиболее остро стоит вопрос о создании единого универсального механизма обеспечения международной информационной безопасности, что прямо следует из положений итоговых документов профильных рабочих групп экспертов ООН. В современных условиях мирового кризиса особенно очевидно, что уровень развития международно-правового регулирования сферы международной информационной безопасности несмотря на ее значимость, по-прежнему неадекватен. В ситуации, когда универсальный механизм не утвержден, особую роль в

регулировании изучаемых отношений играют альтернативные инструменты, которые, хотя и не обладают обязательным характером, тем не менее, могут оказывать значительное влияние на формирование норм и принципов в области информационной безопасности на глобальном уровне. Кроме того, существенную роль играют международные стандарты, рекомендации и практики, разработанные различными международными организациями. Эти документы могут стать основой для разработки национальных стратегий и политик в области информационной безопасности, а также для согласования действий государств на глобальном уровне. Тем самым, несмотря на отсутствие юридически обязательных актов, существует ряд альтернативных механизмов, которые могут способствовать укреплению международной информационной безопасности и содействовать сотрудничеству государств в этой сфере.

Заключение

В завершении исследования представляется необходимым акцентировать внимание на следующих основных выводах.

Информационное общество – это социологическая и футурологическая концепция, которая рассматривает производство и использование научной, технической и другой информации как неотъемлемую часть общественного развития. Концепция информационного общества – это своего рода разновидность теории постиндустриального общества.

В основе российской концепции информационной безопасности лежит представление о ней как о неотъемлемой части национальной безопасности.

Российские правовые нормы в области информационной безопасности распространяются на следующие области:

- специальные режимы защиты информации, требующие реализации определенных мер кибербезопасности (например, защита персональных данных или защита государственной тайны);
- ограничения для операторов связи (например, требование хранить данные о коммуникациях в течение определенного периода времени);
- требования кибербезопасности, применимые к критической информационной инфраструктуре;
- ряд статей уголовного закона России, которые де-факто вводят дополнительные ограничения (например, запрет на создание компьютерных вирусов и кибермошенничество);
- отдельные системы кибербезопасности, созданные частными компаниями, с учетом общих ограничений, предусмотренных законодательством и др.

В учебной литературе информационная безопасность рассматривается как защита информации и защита от информации. При этом дифференциация информационной безопасности на указанные виды является общепризнанной

в науке. Тем самым, термин «информационная безопасность» применяется для обозначения двух различных понятий. Информационная безопасность в первом случае рассматривается в качестве практики предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это понятие обладает универсальностью – применяется независимо от формы, которую могут принимать сведения (электронная/физическая). Основной задачей обеспечения информационной безопасности с этой позиции является сбалансированная защита конфиденциальности, целостности и доступности информации. Тем самым, речь идет о защите данных, о мерах, принимаемых организацией для защиты различных типов информации. Важность этого направления деятельности определяется растущим числом угроз, связанных с цифровизацией различных сфер жизни общества, широким использованием информационных технологий и т.д.

Кроме того, термин «информационная безопасность» используется при изучении проблем безопасности личности. С позиции личностно ориентированного подхода изучаемый термин интерпретируется в качестве состояния защищенности личности, которое обеспечивает ее целостность как активного социального субъекта и возможности развития в условиях информационного взаимодействия с окружающей средой. Актуальность этого направления связана с увеличением числа и диапазона угроз, связанных с влиянием различных источников информации, возникновением феномена «информационной социализации» и др.

Информационная угроза представляет собой определенное воздействие лицом или группой лиц на информационную систему для нанесения ущерба гражданам, обществу и государству.

В исследовании были выделены три вида глобальных информационных угроз, которые могут причинить существенный вред государству.

Во-первых, применение искусственного интеллекта в ходе установления предполагаемых жертв, уязвимостей программ, осуществления

кибератак. При использовании возможностей искусственного интеллекта кибератаки становятся глобальными и наиболее изощренными, с причинением более серьезного ущерба. В современный период искусственный интеллект применяется в ходе создания реальных изображений и звуков. Применение таких инновационных технологий может, например, способствовать получению автомобилям-беспилотниками изображений людей-пешеходов, автомобилей в разнообразной обстановке без выезда при этом на проезжую часть. Применение синтезатора речи определенного человека может повлечь ситуацию, когда пользователь перейдет по ссылке, имеющей компьютерный вирус, или закачает необходимое для преступника электронное приложение.

Следует выделить три вида глобальных информационных угроз, которые могут причинить существенный вред государству:

– применение искусственного интеллекта в ходе установления предполагаемых жертв, уязвимостей программ, осуществления кибератак. При использовании возможностей искусственного интеллекта кибератаки становятся глобальными и наиболее изощренными, с причинением более серьезного ущерба. В современный период искусственный интеллект применяется в ходе создания реальных изображений и звуков. Применение таких инновационных технологий может, например, способствовать получению автомобилям-беспилотниками изображений людей-пешеходов, автомобилей в разнообразной обстановке без выезда при этом на проезжую часть. Применение синтезатора речи определенного человека может повлечь ситуацию, когда пользователь перейдет по ссылке, имеющей компьютерный вирус, или закачает необходимое для преступника электронное приложение;
– применение искусственного интеллекта в политике способствует возникновению манипуляций общественным мнением. При помощи

искусственного интеллекта можно создать фейковую информацию в больших количествах, в результате чего пользователю информации довольно сложно отличить достоверные сведения от ложных данных. В результате предоставления недостоверных сведений повышается адресность пропаганды. С применением возможностей искусственного интеллекта злоумышленники изучают поведенческие основы человека, которые впоследствии могут быть использованы в ходе манипуляций массовым сознанием;

– осуществление кибератак на различные объекты. Данные атаки могут быть применены в ходе массового использования беспилотников или других автоматизированных боевых комплексов. Могут возникнуть возможности незаконного внедрения в системы беспилотных автомобилей вредоносных программ для последующего проведения аварий и различных нападений.

Во-вторых, применение искусственного интеллекта в политике способствует возникновению манипуляций общественным мнением. При помощи искусственного интеллекта можно создать фейковую информацию в больших количествах, в результате чего пользователю информации довольно сложно отличить достоверные сведения от ложных данных. В результате предоставления недостоверных сведений повышается адресность пропаганды. С применением возможностей искусственного интеллекта злоумышленники изучают поведенческие основы человека, которые впоследствии могут быть использованы в ходе манипуляций массовым сознанием.

В-третьих, осуществление кибератак на различные объекты. Данные атаки могут быть применены в ходе массового использования беспилотников или других автоматизированных боевых комплексов. Могут возникнуть возможности незаконного внедрения в системы беспилотных автомобилей вредоносных программ для последующего проведения аварий и различных нападений.

Очевидно, что рост информационных угроз кибербезопасности влечет необходимость поиска механизмов противодействия применению информационных технологий в преступных действиях. Как представляется, основными мерами противодействия современным информационным угрозами должны выступать:

- развитие и дальнейшее функционирование системы постоянного мониторинга информационных систем для обеспечения национальной безопасности государства;
- выработка органами государственной власти и дальнейшее принятие государственных решений по предупреждению информационных угроз объектам безопасности;
- создание моделей устойчивого социального развития информационной системы в различных ситуациях.

Российское законодательство отражает постепенное формирование правовой базы для регулирования отношений в данной сфере, однако стремительное развитие информационных и телекоммуникационных технологий, особенно Интернета, не позволяет своевременно обновлять, вносить изменения и дополнения в правовую базу. Сама сфера рассматриваемых отношений сложна для регулирования в силу множества причин:

- современные средства защиты информации часто неадекватны текущим вызовам и угрозам информационной безопасности;
- многообразие и разнообразие способов совершения правонарушений, преступлений в сети Интернет;
- сложность выявления и отслеживания нарушений законодательства в сети Интернет.

В настоящее время в России приняты документы, которые определяют стратегический подход государства к защите государственных интересов в целом, например, Доктрина информационной безопасности. Вектор развития законодательства в отдельных отраслях обозначен в соответствующих

Стратегиях. Кроме того, принимаются многочисленные федеральные законы, которые часто не предвосхищают, а, наоборот, являются реакцией на уже происходящие события (к моменту принятия законодательный акт в рассматриваемой сфере нередко утрачивает свою актуальность). Регулирование отношений в сфере информационно-коммуникационных технологий должно в равной степени защищать интересы государства, бизнеса и граждан. Однако сегодня оно сводится в основном к введению запретов и ограничений, которые не только не способствуют технологическому развитию страны, но и серьезно его тормозят. В этой связи законодательному регулированию в изучаемой сфере необходим принципиально новый подход.

Развитие информационно-коммуникационных технологий ставит перед государством задачу создания для несовершеннолетних лиц, как наиболее уязвимой категории населения (в силу возраста, психической незрелости и отсутствия жизненного опыта), безопасной информационной среды. Стратегическая цель государства состоит в создании условий для гармоничного развития подрастающего поколения, нейтрализации рисков и угроз, обусловленных стремительным развитием информационно-коммуникационных технологий. Обеспечение безопасной информационной среды для детей требует совместных усилий родительской общественности, образовательных организаций, государственных структур и технологических компаний. Осведомленность, информационная культура и технологические инструменты в комплексе играют ключевую роль в защите детей от информационных угроз.

Текущее правовое регулирование обеспечения информационной безопасности несовершеннолетних в России довольно разнообразно. На федеральном уровне приняты законодательные акты, определившие основные понятие в изучаемой сфере, субъектный состав и содержание отношений по обеспечению информационной безопасности детей, меры ответственности за нарушение законодательных требований и т.д.

Региональные органы власти, в рамках предоставленных им полномочий, самостоятельно определяют мероприятия по обеспечению информационной безопасности детей, опираясь на положения Концепции информационной безопасности детей. Регулирование отношений в этой сфере на уровне регионов обладает определенной спецификой. Региональные нормативные правовые акты могут устанавливать собственные критерии определения деструктивного контента и содержать правовые механизмы его ограничения и др.

Сегодня важность и значимость подготовки нормативных оснований регулирования информационной сферы и обеспечения ее безопасного развития признается практически всеми государствами. В настоящее время наиболее остро стоит вопрос о создании единого универсального механизма обеспечения международной информационной безопасности, что прямо следует из положений итоговых документов профильных рабочих групп экспертов ООН. В современных условиях мирового кризиса особенно очевидно, что уровень развития международно-правового регулирования сферы международной информационной безопасности несмотря на ее значимость, по-прежнему неадекватен. В ситуации, когда универсальный механизм отсутствует, особую роль в регулировании изучаемых отношений играют альтернативные инструменты, которые, хотя и не обладают обязательным характером, тем не менее, могут оказывать значительное влияние на формирование норм и принципов в области информационной безопасности на глобальном уровне. Тем самым, несмотря на отсутствие юридически обязательных актов, существует ряд альтернативных механизмов, которые могут способствовать укреплению международной информационной безопасности и содействовать сотрудничеству государств в этой сфере.

Список используемой литературы и используемых источников

1. Актуальные киберугрозы: итоги 2023 года. // Positivetechnologies: [Электронный ресурс]. Режим доступа. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2/ (дата обращения: 08.04.2024).
2. Баринов С. В. О правовом определении понятия «Информационная безопасность личности» // Актуальные проблемы российского права. 2016. №4 (65).
3. Богатырева Ю.И. Подготовка будущих педагогов к обеспечению информационной безопасности школьников: автореферат дис. ... доктора педагогических наук: 13.00.08 / Ю.И. Богатырева.– Тула, 2014. – 47 с.
4. Бойко С. Основы государственной политики Российской Федерации в области международной информационной безопасности: регулирование и механизмы реализации // Международная жизнь. 2018. № 11.
5. Городнова А. А. Развитие информационного общества: учебник и практикум для вузов / А. А. Городнова. 2-е изд., перераб. и доп. М.: Издательство Юрайт, 2024. 294 с.
6. Договор о сотрудничестве государств – участников СНГ в борьбе с терроризмом от 4 июня 1999 г. Доступ из справ.-прав. системы «Консультант Плюс».
7. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) // Российская газета. № 187. 28.09.2000. Документ утратил силу.
8. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.
9. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности. 4 декабря 1998 г. Документы

Организации Объединенных Наций. Электронный ресурс. Режим доступа. https://documents.un.org/doc/undoc/gen/n99/760/05/pdf/n9976005.pdf?token=fGoARdRNi8YQQheSCB&fe=true (дата обращения 12.04.2024)

10. Жаров А.С. Конституционно-правовое регулирование информационной безопасности личности в Российской Федерации: автореф. дис. … канд. юрид. наук. М., 2006. 26 с.

11. Женевская декларация принципов «Построение информационногообщества – глобальная задача в новом тысячелетии» от 12 декабря 2003 г. Доступ из справ.-прав. системы «Консультант Плюс».

12. Закон РФ от 21.07.1993 № 5485-1 (ред. от 04.08.2023) «О государственной тайне» // Собрание законодательства РФ. 1997. № 41. Ст. 8220-8235.

13. Зенков А.В. Информационная безопасность и защита информации: учебное пособие для вузов. М.: Издательство Юрайт, 2024. 107 с.

14. Илюшенко В. Н. Информационная безопасность общества / Учеб. пособие для вузов. Томск: Томский государственный университет систем управления и радиоэлектроники, 1998. 64 с.

15. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981) // Собрание законодательства РФ. 2014. № 5. Ст. 419.

16. Конвенция о киберпреступности от 23 ноября 2001 г. и протоколы к ней. Доступ из справ.-прав. системы «Консультант Плюс».

17. Конвенция о правах ребенка (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990) // Сборник международных договоров СССР. Выпуск XLVI, 1993.

18. Конвенция ШОС по противодействию экстремизму от 9 июня 2017 г. Доступ из справ.-прав. системы «Консультант Плюс».

19. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Официальный текст Конституции

РФ с внесенными поправками от 14.03.2020 опубликован на Официальном интернет-портале правовой информации http://www.pravo.gov.ru, 04.07.2020.

20. Крутских А.В., Зиновьева Е.С. Международная информационная безопасность: подходы России. М.: МГИМО МИД России, 2021. С. 6.

21. Луман Н. Дифференциация / Пер. с нем.: Б. Скуратов. М.: Издательство «Логос», 2006. 320 с.

22. МСЭ. 2020. Руководство для родителей и педагогов по защите детей в Интернете. Электронный ресурс. Режим доступа. https:// www.иту.int/en/ITU-D/Cybersecurity/Pages/COP-2020-Guidelines.aspx (дата обращения 01.04.2024)

23. Национальная безопасность: учебник / Под ред. Н.Д. Эриашвили, О.А. Мироновой, Е.Н. Хазова. — Москва: ЮНИТИ-ДАНА, 2017. 287 с.

24. Нуянзин С.В., Нуянзин О.С. Информационная безопасность личности и некоторые организационно-правовые меры по ее обеспечению // Юридическая наука и правоохранительная практика. 2018. №2 (44).

25. О внесении в Специальный комитет ООН российского проекта универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях // Министерство иностранных дел Российской Федерации. 2021. 28 июля. Электронный ресурс. Режим доступа. https://archive.mid.ru/foreign_policy/news/asset_publisher/cKNonkJE02Bw/content/id/4831832 (дата обращения: 27.04.2024).

26. Окинавская хартия Глобального информационного общества от 22 июля 2000 г. Доступ из справ.-прав. системы «Консультант Плюс».

27. Полякова Т.А., Шинкарецкая Г.Г. Проблемы формирования системы международной информационной безопасности в условиях трансформации права и новых вызовов и угроз // Право и государство: теория и практика. 2020. № 10. С. 138.

28. Постановление Правительства РФ от 02.06.2008 № 418 (ред. от 15.03.2024) «О Министерстве цифрового развития, связи и массовых

коммуникаций Российской Федерации» // Собрание законодательства РФ. 2008. № 23. Ст. 2708.

29. Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 16.11.2023) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций») // Собрание законодательства РФ. 2009. № 12. Ст. 1431.

30. Приказ Роскомнадзора от 21.02.2013 № 169 (ред. от 09.03.2022) «Об утверждении Порядка получения доступа к содержащейся в единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» информации оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет» // Российская газета. № 74. 05.04.2013.

31. Распоряжение Правительства РФ от 28.04.2023 № 1105-р «Об утверждении Концепции информационной безопасности детей в Российской Федерации и признании утратившим силу Распоряжения Правительства РФ от 02.12.2015 № 2471-р» // Собрание законодательства РФ. 2023. № 19. Ст. 3481.

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

33. Расторгуев С. П. Основы информационной безопасности / Учеб.пособие для студ. высших учебных заведений. М.: Издательский центр «Академия», 2009. 192 с.

34. Роберт И.В. Современное состояние информатизации отечественного образования: фундаментальные и прикладные исследования

// Сборник материалов международной научно-практической конференции «Информатизация образования – 2017». Издательство: Чувашский государственный педагогический университет им. И.Я. Яковлева. Чебоксары, 2017. С. 23- 49.

35. Соглашение между правительствами государств – членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. Доступ из справ.-прав. системы «Консультант Плюс».

36. Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности от 30 ноября 2017 г. Доступ из справ.-прав. системы «Консультант Плюс».

37. Солдатова Г., Чекалина А. Интернет глазами детей и подростков мегаполиса // Дети в информационном обществе. 2009. № 1.

38. Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 07.02.2008 № Пр-212). Доступ из справ.-прав. системы «Консультант Плюс». Документ утратил силу.

39. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. – 2-е изд., перераб. и доп. М.: Издательство Юрайт, 2024. 277 с.

40. Тамодлин, А.А. Государственно-правовой механизм обеспечения информационной безопасности личности: автореф. дис. ... канд. юрид. наук: 12.00.01 / А.А. Тамодлин ;Сарат. юрид. ин-т МВД РФ. Саратов., 2006. 23 с.

41. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 06.04.2024) // Собрание законодательства РФ. 2002. № 1 (ч. 1). Ст. 3.

42. Тунисская программа для информационного общества от 15 ноября 2005 г. Доступ из справ.-прав. системы «Консультант Плюс».

43. Указ Президента РФ от 01.06.2012 № 761 «О Национальной стратегии действий в интересах детей на 2012 – 2017годы» // Собрание законодательства РФ. 2012. № 23. Ст. 2994.

44. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

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

46. Указ Президента РФ от 07.08.2004 № 1013 (ред. от 15.01.2024) «Вопросы Федеральной службы охраны Российской Федерации» // Собрание законодательства РФ. 2004. № 32. Ст. 3314.

47. Указ Президента РФ от 11.08.2003 № 960 (ред. от 27.02.2023) «Вопросы Федеральной службы безопасности Российской Федерации» // Собрание законодательства РФ. 2003. № 33. Ст. 3254.

48. Указ Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Собрание законодательства РФ. 2021. № 16 (Часть I). Ст. 2746.

49. Указ Президента РФ от 16.08.2004 № 1085 (ред. от 08.11.2023) «Вопросы Федеральной службы по техническому и экспортному контролю» // Собрание законодательства РФ. 2004. № 34. Ст. 3541.

50. Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет») // Собрание законодательства РФ. 2015. № 21. Ст. 3092.

51. Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об

информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2019. № 18. Ст. 2214.

52. Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности». Официальный интернет-портал правовой информации http://pravo.gov.ru, 14.07.2022.

53. Федеральный закон от 24.07.1998 № 124-ФЗ (ред. от 28.04.2023) «Об основных гарантиях прав ребенка в Российской Федерации» // Собрание законодательства РФ. 1998. № 31. Ст. 3802.

54. Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2017. № 31 (Часть I). Ст. 4736.

55. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 12.12.2023) «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

56. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

57. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.04.2023) «О защите детей от информации, причиняющей вред их здоровью и развитию» // Собрание законодательства РФ. 2011. № 1. Ст. 48.

58. Цифровая трансформация: вызовы праву и векторы научных исследований: Моногр. / Под общ.ред. А.Н. Савенкова; Отв. ред. Т.А. Полякова, А.В. Минбалеев. М.: РГ-Пресс, 2021.

59. Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г. Доступ из справ.-прав. системы «Консультант Плюс».

60. Шпак А.А. Современные угрозы информационной безопасности // Современное право. 2024. № 1. С. 106 – 108.

61. ManagedDetectionandResponse – 2023. Центр мониторинга кибербезопасности «Лаборатории Касперского». Электронный ресурс. Режим доступа. https://www.kaspersky.ru/about/press-releases/2024_laboratoriya-kasperskogo-v-2023-godu-naibolee-atakuemymi-otraslyami-stali-promyshlennost-finansy-i-it (дата обращения 09.04.2024)