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 «Правовая политика в сфере информационной безопасности»

Обучающийся А.Н. Балдуева
(Инициалы Фамилия) (личная подпись)

Руководитель кандидат юридических наук, И.А. Александров
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2024

Аннотация

Проблема обеспечения информационной безопасности приобретает особую актуальность в связи с наблюдаемым в последние годы усилением угроз информационной сфере Российской Федерации. В частности, речь идет о существенном увеличении количества кибернетических атак, направленных на критически важные информационные ресурсы, активизации деятельности иностранных спецслужб, осуществляющих разведывательную деятельность на территории Российской Федерации, а также о распространении заведомо недостоверной информации, вводящей в заблуждение пользователей. Особую опасность представляет анонимность, присущая электронно-цифровой среде, которая создает благоприятные условия для совершения преступлений, характеризующихся высокой степенью общественной опасности. К ним относятся, в частности, финансирование террористической деятельности, легализация доходов, полученных преступным путем, а также распространение наркотических средств и психотропных веществ. В последнее время наблюдается рост числа обращений в органы МВД, поступающих от родственников граждан, оказавшихся под влиянием деструктивных организаций и сект. В этой связи, важнейшей задачей органов МВД России является обеспечение эффективного предотвращения и профилактики преступлений, в том числе и в сфере общественных отношений, затрагивающих вопросы информационной безопасности.

Целью исследования является определение роли и значения информационной политики в сфере государственного управления и национальной безопасности.

Объект исследования – общественные отношения, возникающие в процессе реализации государством политики по обеспечению информационной безопасности. Предмет исследования – правовые нормы различных отраслей права, регулирующие обеспечение информационной безопасности как составляющей национальной безопасности страны.

Оглавление

Введение

В настоящее время тема обеспечения национальной безопасности на фоне нестабильной политической обстановки в мире приобретает все большее значение и волнует многих. В подтверждение хотелось бы привести слова Владимира Владимировича Путина, сказанные на оперативном совещании с членами Совета Безопасности Российской Федерации: «В нашей повестке дня сегодня вопрос важный, а в условиях сегодняшнего дня - чрезвычайно важный. Речь идет об информационной безопасности России».

В свете недавнего исследования, проведенного Национальным координационным центром по компьютерным инцидентам, неоспоримо установлено, что частота кибернетических посягательств в 2023 году достигла тревожных масштабов. Это явственное свидетельство того, как угрозы информационной безопасности приобретают всевозрастающую роль в формировании экономической обстановки как на государственном, так и на корпоративном уровне. В ответ на данное явление заметна тенденция роста внедрения организациями различных механизмов защиты информации. Одновременно с этим наблюдается значительное увеличение объемов инвестиций в обеспечение кибербезопасности. Тем не менее, несмотря на принимаемые меры, неизменно растет объем убытков, вызванных утратой или неправомерным использованием данных.

Несмотря на очевидные последствия информационных атак представляется весьма затруднительным для количественная оценка. Более того, часть организаций предпочитает утаивать информацию о нарушениях информационной безопасности, если только их раскрытие не влечет юридических последствий, связанных с похищением коммерческой тайны.

Актуальность проблемы информационной безопасности обусловлена, в частности, возрастающей интенсивностью кибернетических атак на информационные ресурсы Российской Федерации, активизацией

деятельности иностранных разведывательных служб, а также распространением заведомо недостоверной информации, вводящей в заблуждение субъектов информационных отношений. Особую сложность представляет анонимность использования информационных ресурсов в электронно-цифровой среде, которая предоставляет широкие возможности для совершения преступлений, в том числе, но не ограничиваясь, финансированием терроризма, легализацией преступных доходов, распространением наркотических средств и психотропных веществ. Следует отметить, что данная проблематика находит отражение в ряде федеральных государственных документов, которые акцентируют внимание на информационных угрозах и мерах по их предотвращению.

Динамичное развитие информационно-коммуникационных технологий неизбежно сопровождается расширением возможностей их недобросовестного использования, что, в свою очередь, создаёт угрозы информационной безопасности и способно приводить к нарушению прав и свобод человека. В последние годы органы МВД России фиксируют рост количества заявлений от родственников граждан, подвергшихся негативному влиянию деструктивных объединений, активно использующих современные информационные технологии для достижения своих целей. В этой связи, предотвращение и профилактика правонарушений, связанных с использованием информационно-коммуникационных технологий, приобретают особую значимость и становятся ключевыми направлениями деятельности органов внутренних дел.

Важно подчеркнуть, что всемирная сеть Интернет в современных условиях стала для многих граждан основным источником информации, вытесняя традиционные средства массовой информации, такие как телевидение, печатные издания, и существенно модифицируя коммуникационные процессы. Общение с родственниками и друзьями все чаще осуществляется посредством мессенджеров и социальных сетей, что свидетельствует о трансформации способов взаимодействия в обществе.

Информационная политика в качестве объекта научного исследования является предметом пристального внимания со стороны исследователей различных научных дисциплин. Необходимо отметить, что в последние годы наблюдается усиление научного интереса к данной тематике, что обусловлено стремительным развитием информационных технологий и их всепроникающим влиянием на все сферы жизнедеятельности современного общества.

В контексте обеспечения национальной безопасности особую значимость приобретает исследование информационной политики как неотъемлемой составляющей системы государственного управления. Следует отметить, что данная сфера в настоящее время находится в начальной стадии освоения в рамках научных исследований. Отсутствие комплексных научных работ, посвященных информационной политике в контексте национальной безопасности, представляет собой объективную реальность, требующую незамедлительного решения.

Целью исследования является определение роли и значения информационной политики в сфере государственного управления и национальной безопасности.

Данная цель определяет постановку следующих задач:

- рассмотреть понятие и роль информационной безопасности в системе национальной безопасности;
- охарактеризовать информационную политику и ее роль в управлении государством и обеспечении национальной безопасности;
- дать общую характеристику и рассмотреть виды информационных угроз;
- проанализировать правовое противодействие современным вызовам и угрозам информационной безопасности;
- обозначить уголовно-правовые и криминологические механизмы обеспечения информационной безопасности;

– выявить проблемы обеспечения кибербезопасности в РФ в условиях цифровизации системы государственного управления и реализации политики в области информационной безопасности.

Объект исследования – общественные отношения, возникающие в процессе реализации государством политики по обеспечению информационной безопасности. Предмет исследования – правовые нормы различных отраслей права, регулирующие обеспечение информационной безопасности как составляющей национальной безопасности страны.

Научная новизна исследования заключается в комплексном изучении роли информационной политики как в управлении государством, так и формировании национальной безопасности, которая является неотъемлемым условием сохранения устойчивости государственной власти и самого государства в целом.

В ходе исследования были использованы материалы научных трудов отечественных и зарубежных исследователей в области права.

Методология. При написании работы использовались следующие методы научного познания: метод анализа и обобщения, логический, формально-юридический методы исследования.

Структура. Работа состоит из введения, трех глав и шести параграфов, заключения, списка используемых источников и используемой литературы.

Глава 1 Информационная безопасность как составная часть национальной безопасности: общая характеристика

1.1 Понятие и роль информационной безопасности в системе национальной безопасности

Вступив в новое тысячелетие, человечество наблюдает стремительное проникновение информационно-коммуникационных технологий во все сферы жизнедеятельности, что обуславливает формирование глобального информационного общества. Данный процесс сопровождается активным принятием международных правовых актов, нацеленных на регулирование взаимоотношений в сфере информационного обмена. В частности, в Декларации тысячелетия, подписанной в начале XXI века, декларируется принципиальная роль образования, знаний, информационного обмена и эффективного коммуникационного взаимодействия в контексте развития национальной безопасности Российской Федерации, обеспечения прогресса и благосостояния каждого гражданина.

«Сегодня сфера национальной безопасности представляет собой сложное, многогранное явление. Она включает в том числе и комплексный набор представлений о всевозможных угрозах как внутри страны, так и за ее пределами, об их воздействии на государство. Сутью национальной безопасности выступает безопасность личности, общества и государства во многих областях жизни общества, включая информационную сферу (защита от информационных угроз)» [37, с. 115].

В контексте стремительного роста роли информации в жизни общества и государства законодатель уже в 1995 году признал важность процессов информатизации, отразив это в Федеральном законе от 20 февраля 1995 года «Об информации, информатизации и защите информации». Несмотря на отсутствие прямого упоминания понятия «информационная безопасность»,

законодательный акт выделяет термин «обеспечение национальной безопасности в сфере информатизации», что подчеркивает незавершенность процессов создания информационных сетей и систем, а также акцентирует внимание на необходимости защиты национальных интересов в сфере информационных технологий.

«При анализе создаваемой системы правового регулирования информационной безопасности были обнаружены некоторые недостатки, которые связаны с тем, что теоретическая база не совершенна относительно вопросов правового обеспечения информационной безопасности России.

Подобно иным странам, Россия испытывает рост влияния информационного сообщества и рассматривает его роль с точки зрения одного из центральных элементов» [13, с.44].

Как справедливо отмечает Ю.Р. Фарвазова, «государственная информационная безопасность в современных условиях приобретает самостоятельное значение, равнозначное, а для некоторых государств даже превосходящее по значимости ядерную безопасность. Несмотря на наличие негативных последствий информационного противостояния, в которое вовлечена и Российская Федерация, свободный доступ к информации по-прежнему является ключевым фактором жизнедеятельности и прогрессивного развития общества в глобальном контексте» [37, с. 115].

Говоря про информационную безопасность на уровне государства, можно отметить, что это «защита национальных информационных систем и активов от всевозможных угроз образуют систему устойчивости государства, обеспечивают его суверенитет. Также здесь подразумеваются своевременные реакции на разного рода провокации, вызовы в информационной среде. В рамках предоставления информационной безопасности предпринимаются меры по недопущению противозаконного доступа к данным, внесению изменений в данные либо их ликвидации. При этом данные всегда являются открытыми для социальных и государственных нужд» [3, с. 351].

В разное время законодательными актами приводились трактовки относительно информационной безопасности государственного уровня. «Информационная безопасность представляет собой защиту информационной среды общества, способствующая ее созданию, использованию и развитию в интересах граждан, организаций и государства» [12, с.199]. Она выражается в защите государства, общества, личности от угроз в информационной среде.

Современные информационно-коммуникационные технологии оказывают существенное воздействие на сферу личных прав, в особенности на право на неприкосновенность частной жизни, являющееся одним из фундаментальных прав человека. В этой связи обеспечение информационной безопасности личности выступает неотъемлемым элементом защиты неприкосновенности частной жизни, исключая возможность несанкционированного распространения информации или содержания переписки в информационном пространстве, включая интернет. "

«Кроме этого, следует отметить также право на получение информации. Статья 29 Конституции РФ предоставляет каждому свободно искать, получать, предавать, производить и распространять информацию любым законным способом. Информационная безопасность в этом случае выступает гарантией того, что граждане имеют доступ к надёжной и безопасной информации, при этом их личные данные при поиске этой информации защищены» [18, с. 21].

Статья 24 Конституции РФ указывает, что сбор, хранение, использование и распространение информации о личной жизни человека без его согласия не допускаются. Данный запрет означает, что никто не вправе распространять личные данные человека, и что без его согласия информация не сможет распространяться. Более детально защита персональных данных регламентирована Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Современные информационно-коммуникационные технологии оказывают существенное воздействие на сферу личных прав, в особенности на право на неприкосновенность частной жизни, являющееся одним из фундаментальных прав человека. В этой связи обеспечение информационной безопасности личности выступает неотъемлемым элементом защиты неприкосновенности частной жизни, исключая возможность несанкционированного распространения информации или содержания переписки в информационном пространстве, включая интернет.

Данное правовое положение гарантирует информационную безопасность, обеспечивая защиту данных как при их передаче, так и при их хранении в информационных системах, что соответствует принципам конфиденциальности и целостности информации.

«В рамках информационной защиты осуществляется ряд конституционных прав и свобод человека, обеспечивается оптимальный уровень жизни населения, сохраняется суверенитет, целостность территориальных границ, благоприятное развитие в социально-экономическом пространстве, предоставляются гарантии безопасности (п. «в» ст. 3 Доктрины информационной безопасности РФ 2016 г.)» [35].

«Что касается долговременной перспективы, то к интересам России можно причислить такие аспекты, как: экономическая, энергетическая, геополитическая, социокультурная, демографическая, военная, экологическая безопасность (ст.1 ФЗ «Об охране окружающей среды» от 10.01.2002 № 7-ФЗ), инновационное развитие, международное сотрудничество, а также, информационная безопасность» [11, с. 59].

Угрозы национальной безопасности, представляющие собой комплексный феномен, могут быть классифицированы по месту их возникновения, выделяя при этом две категории:

– внутренние угрозы. Данный тип угроз, имеющий своим источником внутреннюю среду государства, зачастую обусловлен конфликтами внутригосударственного характера. К характерным примерам

подобных угроз относятся: социальные потрясения, ведущие к дестабилизации общества, экономические кризисы, вызывающие системные дисфункции, и преступность, нарушающая правопорядок и общественную безопасность;

- внешние угрозы. Эти угрозы, проистекающие из-за пределов государственной территории, могут носить различный характер, включая международные конфликты, способные дестабилизировать региональную обстановку, экономические санкции, применяемые в качестве инструмента политического давления, а также несанкционированную деятельность иностранных государств, направленную на сбор конфиденциальной информации с целью нанесения ущерба национальным интересам. К внешним угрозам также относятся противозаконное размещение вооруженных сил иностранных государств в пограничных зонах, несоблюдение условий международных военных соглашений, таких как соглашения о сокращении вооружений, террористические атаки, направленные на подрыв национальной безопасности, кибератаки, осуществляемые с целью нанесения ущерба информационным системам, и проявления агрессии в любой другой форме.

Таким образом, «информационная безопасность, представляет собой систему мер и средств, направленных на обеспечение конфиденциальности, целостности, доступности и надежности информации, а также на защиту информационных ресурсов и информационной инфраструктуры от различных

угроз и рисков, включая киберугрозы, с целью обеспечения интересов личности, общества и государства. Она напрямую связана с обеспечением национальных интересов государства. Среди таких интересов могут быть экономическая стабильность, политическая независимость, обороноспособность, социокультурное развитие и другие. Информационная безопасность необходима для обеспечения нормальной работы

государственных органов и организаций; манипуляции в информационной сфере могут влиять на общественное мнение и политическую ситуацию в стране. Фальсификация информации или дезинформация могут создавать конфликты и нестабильность. Информационная безопасность также важна для обороноспособности государства. На международной арене уровень информационной безопасности государства влияет на его международные отношения и сотрудничество. Угрозы в информационной сфере могут непосредственно подрывать все перечисленные интересы» [15, с. 50].

В контексте стремительной цифровизации современного общества вопрос обеспечения безопасности информационных систем приобретает особую актуальность. Информационные системы, хранящие и обрабатывающие сведения, оказывают существенное влияние на безопасность как физических лиц, так и общества в целом, а также на национальную безопасность государства.

«В число таких систем, помимо прочих, входят:

- системы связи и телекоммуникаций;
- системы хранения и обработки персональных данных;
- объекты критической инфраструктуры, включая, но не ограничиваясь, атомные электростанции;
- системы управления наземным и воздушным транспортом;
- банковские информационные системы;
- системы формирования общественного мнения» [28, с. 15].

Обеспечение бесперебойной и надежной работы указанных информационных систем требует неукоснительного соблюдения принципов информационной безопасности, направленных на сохранение их целостности, конфиденциальности и доступности.

Отсутствие надлежащей защиты информационных систем может привести к:

- несанкционированному доступу к конфиденциальной информации;

– разрушению или модификации данных, что может привести к финансовым потерям, ущербу репутации и другим негативным последствиям;
– нарушению функционирования критически важных объектов инфраструктуры, что может повлечь за собой угрозу общественной безопасности;
– дестабилизации информационного пространства и манипулированию общественным мнением.

«В рамках государственной политики в сфере информационной безопасности ключевую роль играет государственно-правовое направление. Оно тесно связано с функционированием органов государственной власти, состоянием законодательной и нормативно-правовой базы, а также с уровнем развития «человеческого фактора», потенциала и общественных отношений» [2, с. 315].

Одним из основополагающих документов в сфере информационной безопасности является Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [36]. Проанализировав текст данного документа, можно выделить основные задачи, принципы и направления государственной политики в сфере информационной безопасности Российской Федерации, поставленные перед федеральными органами государственной власти, органами власти субъектов РФ, общественными организациями: «Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами».

В современных условиях наблюдается тенденция к интенсификации правонарушений, в том числе в сфере информационных технологий, что обуславливает необходимость обеспечения информационной безопасности.

В целях комплексного решения задач, связанных с развитием информационного общества и защитой прав граждан в информационной сфере, Президентом Российской Федерации в 2017 году была подписана Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы.

Данная Стратегия предусматривает реализацию следующих ключевых направлений:

- «обеспечение прав граждан на доступ к информации, гарантируя свободный и беспрепятственный доступ к достоверной и актуальной информации в соответствии с законодательством Российской Федерации;
- обеспечение государственной защиты интересов граждан в информационной сфере, включая защиту от незаконного сбора, хранения, использования и распространения информации о гражданах, а также от информационного воздействия, угрожающего национальной безопасности и общественному порядку;
- обеспечение законности в процессе сбора, хранения и распространения информации о гражданах и организациях, устанавливая строгие требования к процедурам обработки персональных данных, предусматривая правовую ответственность за нарушение законодательства в этой области» [2].

«Проблема обеспечения информационной безопасности Российской Федерации имеет комплексный характер, поэтому для ее решения государство сочетает правовые, организационные и технические меры.

Правовые меры обеспечения информационной безопасности предполагают задействование норм разных отраслей права. Данные меры направлены на разработку различных нормативно-правовых актов, регулирующих отношения между субъектами в информационной сфере.

Организационные меры предполагают модернизацию методов информационной защиты, методов управления системой информационной безопасности и ее структуры.

Технические меры включают действия, направленные на предотвращение информационной утечки, уничтожения или искажения хранящейся информации. Это осуществляется путем ограничения каких-либо воздействий, которые могут привести к сбоям в информационной системе, а также посредством активного применения усиленных средств защиты информации» [2, с. 315].

В основе концепции информационной безопасности лежит защита трех ключевых свойств информации:

- конфиденциальности;
- целостности;
- доступности.

Конфиденциальность информации подразумевает ограничение круга субъектов, наделенных правом доступа к ней, исключительно лицами, определенными владельцем информационного ресурса. Нарушение конфиденциальности наступает в случае получения доступа к защищенным данным неуполномоченными лицами, что влечет за собой несанкционированное разглашение конфиденциальной информации.

Целостность информации, как фундаментальный принцип информационной безопасности, предполагает сохранение ее неизменного состояния. Повреждение целостности происходит при неправомерных изменениях информационного ресурса, как в результате случайных сбоев, так и в результате преднамеренных действий, направленных на искажение или модификацию исходных данных. Особую важность приобретает сохранение целостности данных, непосредственно влияющих на функционирование критически важных инфраструктурных объектов, поскольку их изменение может привести к негативным последствиям для общества.

Доступность информации определяется возможностью авторизованных пользователей своевременно получать к ней доступ. Потеря доступности наступает в случае блокирования или уничтожения информации, как в результате случайных событий, так и в результате преднамеренных действий, направленных на ограничение или прекращение доступа к информационным ресурсам.

Одной из проблем, которая стоит перед органами государственной власти России, является обработка больших данных. К сожалению, зачастую не хватает ресурсов для обеспечения безопасного хранения информации. Как отмечают исследователи, «несмотря на то, что большие данные в их классическом понимании есть совокупность технологий, которые призваны обрабатывать большие по сравнению со «стандартными" сценариями объемы данных и работать со структурированными и плохо структурированными данными параллельно в разных аспектах, когда разговор заходит о законодательном регулировании, большие данные рассматриваются в первую очередь в контексте проблематики персональных данных» [4, с. 51]. «Это связано в первую очередь с тем, что сбор и обработка данных в сети порождают проблемы, сопряженные с защитой личных данных граждан. По сети Интернет рассредоточено множество информации о гражданах России. Зачастую она носит открытый характер, т. е. такую информацию пользователь указывает сам. Однако, несмотря на открытый характер информации, все равно остается проблема отсутствия правового статуса информации, собранной в сети Интернет. А это, в свою очередь, нарушает право граждан на неприкосновенность частной жизни, предусмотренное Конституцией Российской Федерации» [3, с. 353].

Для эффективного решения проблемы сбора информации о пользователях в сети необходимо четкое законодательное определение границ сбора, обработки и передачи данных. Необходимость подобного регулирования обусловлена необходимостью обеспечения баланса между интересами пользователей в защите персональных данных и интересами

операторов в получении информации для оптимизации своей деятельности. В Российской Федерации была предпринята попытка законодательного решения данной проблемы. В 2018 году в Государственную думу был внесен законопроект федерального закона № 571124-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»», предполагавший установление строгого порядка сбора, передачи и обработки пользовательских данных. Однако, данный законопроект был возвращен субъекту законодательной инициативы в связи с несоответствием положений части 3 статьи 104 Конституции РФ и статьи 105 Регламента Государственной думы. Это свидетельствует о необходимости более тщательной проработки законопроекта с учетом конституционных норм и регламентных требований для обеспечения его соответствия правовой системе Российской Федерации.

«Следует констатировать, что степень защищенности информационных систем ощутимо отстает от динамично нарастающего числа как внутренних, так и внешних угроз. Увеличение количества последних влечет за собой существенные риски возникновения информационных утечек, а также несанкционированного изменения содержания хранящейся информации. Все это, в конечном итоге, может иметь пагубные последствия для национальной безопасности Российской Федерации.

В условиях сложившейся ситуации обеспечение информационной безопасности государства сталкивается с дефицитом квалифицированных кадров. В целях устранения данного фактора Министерство науки и высшего образования Российской Федерации предпринимает меры по увеличению количества бюджетных мест для абитуриентов, желающих обучаться по специальностям, связанным с информационными технологиями» [23, с. 9].

Исходя из изложенного, очевидно, что одним из приоритетных направлений совершенствования правовой политики России в сфере информационной безопасности является повышение результативности законотворческой деятельности. Введение в действие новых нормативно-

правовых актов позволит адекватно реагировать на вызовы, возникающие в связи с развитием информационных технологий, и обеспечить надлежащий уровень защиты от угроз информационной безопасности.

1.2 Роль информационной политики в управлении государством и обеспечении национальной безопасности

Информационная политика в рамках современного государственного управления представляет собой фактор первостепенной важности, требующий глубокого анализа и комплексного учета при формировании и реализации национальной стратегии развития. Информационная политика - это не материальная, а динамично развивающаяся категория, являющаяся неотъемлемой частью государственной политики. Эффективная информационная политика предполагает от властных структур глубокое понимание тенденций трансформации как видов информации, так и информационных технологий в глобальном масштабе.

«Государство, уделяющее пристальное внимание разработке и реализации информационной политики, а также неукоснительному соблюдению ее основополагающих принципов, приобретает значительный иммунитет к внешним и внутренним факторам, направленным на дестабилизацию гражданского общества и дискредитацию государственных институтов» [24, с. 106].

«Информационное развитие расширяет границы в разных областях жизнедеятельности общества и государства. Оно направляет общественное развитие, позволяет государству оптимизировать и упорядочить процессы управления, а также налаживать общественно-государственный диалог. Однако широкие возможности одновременно несут и высокие риски, преодолеть которые возможно с помощью сочетания инноваций и традиций, а также повышения управляемости с целью контроля информационных потоков и информационного развития общества и государства в целом. Таким

образом, информационная политика является одной из наиболее актуальных областей государственного управления и становится важным аспектом в обеспечении национальной безопасности.

Информационная политика как часть государственной политики Информационная политика – это совокупность всех государственных законов, постановлений и политик, которые поощряют, препятствуют или регулируют создание, использование, хранение, доступ, а также передачу и распространение информации. Она охватывает любую другую практику принятия решений с общеорганизационными усилиями, которые связаны с потоком информации и тем, как она обрабатывается» [17, с. 18].

Информационная политика, являющаяся комплексом мер, направленных на регулирование информационных процессов, опирается на ряд фундаментальных элементов, определяющих ее ключевые направления. Особое место занимает сфера государственной политики, охватывающая использование информации для стимулирования демократических процессов и развития коммерческих отношений в общественной жизни. В рамках этой сферы определяются конкретные механизмы регулирования, касающиеся цифровой среды, интеллектуальной собственности, экономических отношений, свободы выражения мнений, защиты конфиденциальности информации, обеспечения информационной безопасности, управления доступом к информации и регулирования распространения публичной информации.

«Ввиду особой значимости для населения и его информированности о ключевых аспектах жизнедеятельности, отдельные категории информации подлежат приоритетному рассмотрению в рамках информационной политики. К ним относятся:

- новостная информация: обеспечивающая информирование населения о текущих событиях и процессах, оказывающих непосредственное влияние на их жизнь;

– данные о состоянии здоровья населения: необходимые для принятия эффективных мер по сохранению и улучшению общественного здоровья, а также для проведения научных исследований в области здравоохранения;
– информация, собираемая в ходе переписи населения: позволяющая получить объективные данные о демографической ситуации в стране, необходимы для планирования социально-экономического развития, а также для реализации различных государственных программ» [37, с.116].

Указанные категории информации представляют безусловный общественный интерес, поскольку обеспечивают доступ к сведениям о ключевых социально-экономических и демографических процессах, происходящих в обществе.

Информационная политика является одним из центральных элементов функционирования современных информационных обществ. В условиях глобального перехода от индустриализма к постиндустриализму информационные проблемы приобретают все большую актуальность. В частности, обеспечение свободного доступа к достоверной и актуальной информации, а также защита от распространения ложной информации являются ключевыми факторами устойчивого развития общества.

По мнению социологов, «сейчас важна не грубая сила, а информация. В то время как все виды современных обществ в той или иной степени основаны на информации, информационные общества почти полностью зависят именно от компьютеризированной информации. Основой информационной экономики, новым центральным фактом реальности является компьютер. Его способность манипулировать информацией и обрабатывать ее представляет собой фундаментальный отход от человеческих способностей, а сочетание компьютера с телекоммуникациями создает политические проблемы будущего» [5, с. 42].

«Информационная политика стала важной областью изучения во второй половине XX века, когда произошел переход от индустриального общества к информационному. Она превратилась из второстепенной в имеющую всеобъемлющее стратегическое значение, поскольку теперь определяет условия, при которых происходит принятие всех других решений, публичный дискурс и политическая активность» [6, с. 46].

«Хотя информационная политика, как правило, имеет более широкое определение и включает в себя множество компонентов, ее масштабы и воздействие могут варьироваться в зависимости от контекста. Например, в контексте жизненного цикла информации данный вид политики относится к законам, которые касаются трансферных этапов, начиная с ее создания, через ее сбор, организацию, распространение и, наконец, ее уничтожение. С другой стороны, информационная политика позволяет субъектам государственного управления адаптироваться к быстро меняющейся среде и использовать информацию для принятия решений. Можно видеть, что эти два контекста предлагают различные области применения понятия «информационная политика» [6, с. 46].

«Информационная политика представляет собой комбинацию нескольких различных научных областей деятельности общества, включая информатику, экономику, юриспруденцию и государственную политику. Информационные науки сосредоточены на технических достижениях и том, как они влияют на информационную политику, в то время как, например, право на неприкосновенность частной жизни и интеллектуальная собственность являются не менее важной составляющей информационной политики» [9, с. 30].

«Информационная политика, будучи неотъемлемой частью государственной политики, играет ключевую роль в ее функционировании. Государственная политика, в свою очередь, немыслима без систематизированного и структурированного потока информации. Это обусловлено необходимостью предварительного сбора и анализа данных,

которые служат основой для принятия взвешенных решений ответственными лицами, а также для комплексного изучения процессов, направленных на совершенствование политических систем. Важно подчеркнуть, что каждое государство формирует свою политику, руководствуясь уникальными чертами собственной культуры, историческим наследием, актуальными проблемами, потребностями и другими определяющими факторами» [33, с. 23].

Информационная политика государства представляет собой совокупность правовых норм, мер и действий, осуществляемых на государственном уровне, направленных на регулирование информационных отношений, обеспечение информационной безопасности, удовлетворение потребностей различных субъектов в информации и защиту их интересов в информационном пространстве. В контексте национальной безопасности информационная политика выступает как ключевой элемент, определяющий уровень устойчивости и способности государства противостоять внешним и внутренним угрозам, связанным с информационным пространством.

«Комплекс всех проводимых государственных политик – в социальной сфере, сфере политики, экономики, права, культуры – входит в общую систему национальной политики государства, то есть государственная политика является частью общей политики в стране, направленной на решение конкретных вопросов в определенный промежуток времени, что требует оперативности, защищенности и верификации информации, предоставляемой для эффективного функционирования. При этом эффективную государственную политику отличает соответствие четко сформулированным демократическим целям с привлечением к их разработке общества, частного сегмента и профессионалов в каждом обсуждаемом вопросе. Она должна содержать планирование, согласование ресурсов, обсуждение и прогноз результатов и альтернатив» [11, с. 57]. «Государственная политика всегда должна ориентироваться на конъюнктуру в каждой из областей жизнедеятельности, т. к. она направлена на решение конкретных назревших в определенной сфере общественных отношений

проблем и задач. Демократические основы государственной политики предполагают не только многоканальность доступа к информации, но и ее постоянную верификацию на предмет искусственного искажения, альтернативного трактования, подделки в форме дезинформации и удаления из информационного поля. Поэтому государственная политика при продвижении демократической повестки крайне нуждается в хорошо проработанной информационной политике, которая, в свою очередь, соответствует принципам национальной безопасности государства» [10, с. 14].

Отметим, что «основной вектор государственной политики в современной России сменился в период распада Советского Союза и перехода российской экономики от административно-плановой к рыночной модели, а также появилась возможность перенимать опыт передовых западных государств в сфере всей системы государственного управления» [19, с. 30]. «Информационная политика государства вообще не была сформулирована, поэтому позволяла реализовывать не столько транспарентность мнений, сколько комплекс одностороннего влияния на гражданское общество и акторов власти. В дальнейшем активность гражданского общества стала возрастать, что позволило говорить о развитии институтов демократии в государственном управлении. Однако данный процесс не развился в полной мере, т. к. российский национальный менталитет исторически тяготеет к иерархии, бюрократии, централизованной власти и соборности. Нередко бюрократия оказывает гораздо большее влияние на формирование и реализацию государственной политики, чем население» [22, с. 6023]. Так, по мнению некоторых исследователей в России действует так называемая бюрократическая модель принятия решений. Таким образом, историческая траектория формирования российской информационной политики демонстрирует существенные различия с западными моделями, характеризующимися, на первый взгляд, абсолютной свободой прессы и информационных потоков, гарантирующей как право на

неприкосновенность частной жизни, так и право на доступ к информации, признанной общественно или государственно значимой. В российской социокультурной среде сохраняется превалирующий уровень доверия к официальным информационным источникам, генерируемым органами государственной власти. В результате альтернативные информационные потоки постепенно утрачивают статус формальных источников для гражданского общества, воспринимаясь преимущественно как категория развлекательной информации или, в худшем случае, как источник дезинформации. Именно эта тенденция во многом предопределяет механизмы контроля за информационными потоками в целях обеспечения национальной безопасности [21, с. 56].

В современной научной литературе имеется ряд разночтений относительно того, как классифицировать государственную политику. Так, Соколов А. Ю., Лакаев О. А. утверждают, что, «согласно документам и данным из научной литературы, можно выделить более 50 видов государственной политики в различных областях регулирования» [32, с. 92].

Различные авторы придерживаются различных критериев для ее систематизации. В данном исследовании «наиболее релевантным представляется критерий дифференциации государственной политики по сферам и объектам целеполагания, планирования и регулирующего воздействия. Согласно данному критерию, государственная политика подразделяется на следующие категории:

- экономическая политика: включает в себя аграрную, промышленную, налоговую политику и другие ее составляющие;
- социальная политика: охватывает национальную, демографическую, молодежную политику и т.д.;
- политика национальной безопасности: объединяет военную, информационную, правоохранительную политику и другие направления» [8, с. 91].

Таким образом, «в сферу государственной политики национальной безопасности входят военная и информационная политики, которые объединяются общей целью – предотвращением войны.

Информационная политика государства в сфере национальной безопасности направлена на недопущение начала военного конфликта, поскольку война представляет собой угрозу для национального менталитета, что является важным элементом государственного устройства» [6, с. 47].

Как говорилось выше, «одной из важнейших составляющей информационной политики государства является информация. Современная наука дает множество определений категории «информация». Информация – это обозначение содержания, полученного от внешнего мира в процессе приспособления к нему.

Информация – мера сложности структур. Информация – коммуникация и связь, осуществляя которую устраняется неопределенность.

Необходимо уточнить, что ни одно из представленных определений не может считаться правильным или исчерпывающим, т. к. в каждом из них раскрывается определенная специфическая черта полиаспектного явления под названием информация, связанная с той или иной сферой общественной жизнедеятельности, среди которых и политическая сфера.

С прагматической точки зрения, информация – это сведения, которые включаются в имеющиеся данные, предназначенные для практического использования. Информация помогает ее получателю освободиться от неопределенности в процессе принятия решения» [27, с. 181].

«Эффективное функционирование системы государственного управления в условиях информационного общества обусловлено наличием адекватного канала коммуникации, предусматривающего обратную связь между государством и обществом, а также иными субъектами, участвующими в реализации государственной политики в соответствующих сферах. Важнейшим элементом государственной информационной политики выступает обеспечение обратной связи с обществом посредством

налаживания систематического и качественного информационного взаимодействия с различными субъектами, позволяющего выявлять их потребности и запросы. Следовательно, информация, в отличие от простых данных, отличается наличием специфического атрибута - устранения неопределенности, что позволяет определить ее как фактор, способствующий принятию обоснованных и эффективно реализуемых управленческих решений» [28, с. 56].

«Информационная политика государства имеет три объекта в зависимости от поставленных целей:

- все процессы и явления, которые связаны с развитием общества в информационной сфере;
- гарантии и обеспечение свободы массовой информации, которые становятся реальными в результате расширения возможностей для граждан в области доступа к информации;
- возможности технического оснащения граждан, которые расширяют информационную инфраструктуру» [28].

Следовательно, «это требует от государственного управления технологического совершенствования и в то же время модернизации механизмов и методов национальной безопасности, чтобы информационная политика, с одной стороны, развивалась в рамках потребности гражданского общества в доступности информации, а с другой стороны, не становилась оружием влияния внешних сил на представителей данного общества и тем более на такие категории, как молодежь и сотрудники государственного и муниципального аппарата. В связи с этим необходимо уточнить понятие национальной безопасности» [28, с. 57].

Несовершенство информационной политики государства, в контексте анализа угроз национальной безопасности, представляет собой фактор, обладающий потенциалом дестабилизации общественных основ и подрыва основ государственности.

В Российской Федерации, на протяжении более чем трех десятилетий, информационная политика, отличающаяся значительной степенью свободы для разнообразных субъектов информационного производства и сфер влияния, сформировала информационную среду, в которой гражданское общество подвергается воздействию многочисленных информационных источников, интерпретирующих и трактующих информацию различным образом. Такая информационная среда порождает существенные негативные последствия, проявляющиеся в процессах деструктивных социальных трансформаций, утраты национальной идентичности и искажения общественных представлений о реальности. В результате наблюдается дискредитация государственных институтов, что подрывает основы государственности, историческую традицию единства и снижает уровень доверия к власти [1, с. 40].

«В контексте усиливающейся информационной нестабильности, первостепенное значение приобретает разработка и применение действенных механизмов и методов обеспечения национальной безопасности в рамках государственной политики в сфере информации» [1]. Данная задача является приоритетной, определяя не только актуальность, но и устойчивость и существование Российского государства.

Таким образом, для обеспечения устойчивого функционирования государство обязано не только разрабатывать и реализовывать информационную политику, но и осуществлять ее постоянное совершенствование, учитывая как стремительное развитие технологических инноваций, так и фундаментальные национальные принципы, обычаи и традиции. Данная деятельность направлена на сохранение национальной идентичности гражданского общества и формирование мировоззрения, соответствующего государственным интересам.

Глава 2 Основные угрозы информационной безопасности

2.1 Общая характеристика и виды информационных угроз

В завершении XX столетия произошло кардинальное переосмысление роли информации в общественном контексте, что нашло отражение в научных трудах. Бурное развитие коммуникационных технологий, являясь вектором прогресса, одновременно породило новые угрозы, потенциально способные подорвать стабильность мирового и национального развития. Особое значение в этом контексте приобретает концепция информационной безопасности, охватывающая сферы общества, государства и личности. Данная концепция приобретает актуальность на фоне формирования информационного общества, характеризующегося всепроникающим влиянием информационных потоков на все сферы жизнедеятельности. Современные информационные технологии утратили рамки национального суверенитета, обретя глобальное значение. В условиях тотальной информатизации, охватывающей все аспекты жизни, вопросы обеспечения информационной безопасности выходят на первый план, требуя пристального внимания и комплексных мер по их решению.

«Глобализированный мир ставит перед национальными сообществами, государствами и человеком новые вызовы и угрозы, которые интенсифицируются через активизацию глобальных информационных обменов. Перед современным человеком и обществом предстает в этом аспекте сложная дилемма: с одной стороны, информатизация и глобальное информационное пространство дают множество новых возможностей развития в различных сферах общественной жизнедеятельности, а с другой – из-за интенсивности самих информационных потоков и бурного развития технологий информационного обмена, постоянно возникают новые угрозы безопасности человека и общества» [7, с. 90].

«Развитие интернет-технологий обусловило непрерывное возрастание угроз информационной безопасности, выражающихся в применении методов социальной инженерии, несанкционированного доступа к информационным системам, а также в распространении вредоносного программного обеспечения. Следствием реализации подобных угроз в отношении информационных систем государственных учреждений, организаций и коммерческих структур является нанесение ущерба финансовому благополучию, а также утрата ценных данных, являющихся объектом интеллектуальной собственности» [37, с.118].

«Политика безопасности государственных учреждений / организаций / компаний строится на выявлении характеристик, влияющих на поведение пользователей в области информационной безопасности и высокой степени уязвимости к киберугрозам. Важно также учитывать то, что намерения пользователей информационных систем могут отличаться от их фактического поведения. Под социальной инженерей понимают процесс получения доступа к конфиденциальным данным физических или юридических лиц посредствам манипулирования человеческой психологией» [30, с. 17]. Таким образом, конечный пользователь информационной системы является самым слабым звеном.

«Социальная инженерия описывает тип атаки, когда злоумышленник или группа злоумышленников использует уязвимости человека посредством убеждения, обмана, манипулирования, а также побуждения для целей нарушения информационной безопасности.

Анализируя развитие информационных технологий безопасности, можно сделать заключение, что классические технические атаки стали сложными и по этой причине злоумышленники переключились на социальную инженерию. Человеческий фактор присутствует в каждой информационной системе. Он характеризуется уязвимостью и в значительной степени влияет на уязвимость информационной безопасности

государственного учреждения / организации / компании, особенно если атака будет совершаться квалифицированными злоумышленниками» [29, с. 170].

«В настоящее время социальная инженерия способна получать большие объемы конфиденциальной информации и имеет больше каналов атаки посредством различных приложений (социальные сети, интернет-вещей, мобильная связь). Машинное обучение и искусственный интеллект сделал социальную инженерию эффективным и автоматизированным видом угрозы информационной системы. Атаки социальной инженерии стали крупномасштабными и роботизированными.

Таким образом, используя инструмент социальной инженерии, злоумышленники могут достигнуть большой группы целей, тщательно выбрав конкретных жертв» [19, с. 16].

Существуют внешние и внутренние информационные угрозы. Внешние исходят от роботов, мошенников (фишинг и социальная инженерия), хакеров, вредоносного программного обеспечения (ПО), к которым относятся вирусы, троянские программы, шпионское ПО. Самый распространенный пример внешней угрозы – DDoS-атака (от англ. Distributed Denial ofService). DDoS-атака выглядит так, как будто бизнес-сайт одновременно пытаются открыть тысячи пользователей. Из-за большого количества запросов сервер, на котором хранятся файлы сайта, не успевает обрабатывать их и периодически выходит из строя. DDoS-атаки могут привести к отказу в обслуживании сайта и потере доходов. DDoS-атаки могут иметь различные цели: конкуренты могут использовать их для отключения сайта, мошенники – для вымогательства выкупа у владельцев ресурсов.

Внутренние угрозы могут быть: случайными (из-за ошибок сотрудников); намеренными (когда сотрудники намеренно нарушают безопасность, забирая с собой после увольнения часть клиентской базы или продавая ее конкурентам).

«Информационный терроризм еще одна неотъемлемая и актуальная угроза национальной безопасности в современном мире. Развитие

информационных технологий и глобального интернета привело к появлению новых возможностей для экстремистских и террористических организаций в области манипуляции и распространения информации» [20, с. 21].

«В условиях глобализации и стремительного развития информационных технологий, актуальность проблемы информационного терроризма для национальной безопасности неуклонно возрастает. Информационный терроризм представляет собой угрозу национальной безопасности, поскольку основывается на злонамеренном использовании информационных технологий и средств коммуникации с целью распространения заведомо ложной, искаженной или провокационной информации. Такая информация способна нанести существенный вред государству, его гражданам и их законным интересам.

Основная цель информационного терроризма заключается в дестабилизации политической, экономической и социальной обстановки в стране путем создания атмосферы паники, неуверенности и хаоса в обществе» [16].

«Деятельность, квалифицируемая как информационный терроризм, несет в себе значительный потенциал для нанесения ущерба национальной безопасности, оказывая разрушительное воздействие на разнообразные сферы государственной жизни. Осуществление информационного терроризма способствует углублению общественного недоверия к государственным органам власти, порождая конфликты, как межконфессионального, так и межнационального характера, негативно влияя на стабильность экономики и политического устройства страны. Более того, информационный терроризм может быть использован для дискредитации государственных институтов и уничтожения их влияния на общественное сознание.

В целях обеспечения национальной безопасности необходимо прилагать максимальные усилия для предотвращения и противодействия информационному терроризму. Важно укреплять кибербезопасность, разрабатывать законодательство, которое запрещает и наказывает

информационный терроризм, проводить пропаганду и образование населения в области информационной безопасности. Также необходимо укреплять сотрудничество и обмен информацией с другими странами для более эффективной борьбы с этой угрозой» [16, с. 52].

Одним из ключевых элементов информационного терроризма является дезинформация и манипуляция сознанием граждан. Используя средства распространения ложной информации, такие как фейковые новости, поддельные видеоматериалы и манипулятивные комментарии, террористы стремятся создать условия хаоса и нестабильности, а также подорвать доверие к государственным органам и другим институтам власти.

«Особое значение в реализации информационного терроризма играет активное использование социальных сетей, блогов, форумов и других онлайн-платформ. Террористы используют данные каналы для распространения пропагандистской информации, вербовки новых сторонников и формирования информационного влияния. При этом они рассчитывают на эффект «вирусного» распространения, когда одно сообщение или видео могут быстро стать «трендом», достигнув широкой аудитории и оказывая значительное воздействие на общественное мнение» [20].

«Информационный терроризм имеет не только непосредственные последствия, но и долгосрочные. Он способен разжечь межнациональные и межрелигиозные конфликты, основанные на манипуляции информацией, а также способствовать радикализации общества и индивидуальных личностей.

Борьба с информационным терроризмом стала важным приоритетом для государственных и международных организаций. Для эффективного противостояния этой угрозе требуется разработка и реализация комплексных стратегий и политик в области информационной безопасности, в том числе защиты критической информационной инфраструктуры, обучение граждан осознанному использованию информации и фильтрации недостоверных

источников, а также укрепление международного сотрудничества для обмена опытом и информацией» [20, с. 52].

«Информационный терроризм – это серьезная угроза, которая требует всестороннего анализа и принятия соответствующих мер для защиты национальной безопасности. Необходимо постоянное развитие и совершенствование методов противодействия информационным террористам, чтобы обеспечить стабильность, безопасность и целостность общества и государства в информационной эпохе.

Одной из особенностей информационного терроризма является его невидимость и отсутствие физической разрушительной силы, при этом его последствия могут быть катастрофическими» [13, с.55].

Во-первых, «информационный терроризм основывается на использовании различных средств массовой информации, включая интернет, телевидение, радио, социальные сети и прочие цифровые платформы. Проникнув в эти каналы связи, террористы манипулируют информацией, создавая идеологические и политические конфликты, распространяя пропаганду и провокации. С помощью фейковых новостей, дезинформации, хакерских атак и других технологий, они пытаются повлиять на общественное мнение, нарушить стабильность экономики и политической системы страны.

Во-вторых, информационный терроризм характеризуется широким спектром методов и техник, которые используются для достижения своих целей. Это может включать кибератаки на государственные структуры и важные информационные системы, создание вирусов, троянов и других вредоносных программ, а также использование методов социальной инженерии для манипуляции сознанием людей. Применение таких методов позволяет террористам не только нанести ущерб целевой организации или государству, но и создать общественный дисбаланс, страх и панику, что является их целью.

В-третьих, информационный терроризм имеет глобальный характер и не ограничивается границами отдельных стран. С помощью интернета и мировых коммуникаций, террористам удается воздействовать на международную общественность и вызывать нестабильность на региональном и глобальном уровне. Они способны связываться друг с другом, обмениваться опытом и практиками, что делает борьбу с информационным терроризмом особенно сложной и требует глубокого понимания его природы и методов» [14, с. 13].

В целом, «информационный терроризм представляет серьезную угрозу для современного общества, требующую соответствующих мер и приоритетов в области кибербезопасности. Необходимо развивать эффективные стратегии и технологии для выявления и противодействия информационному терроризму, а также пропагандировать информационную грамотность и критическое мышление, чтобы люди могли различать правду от лжи в информационном пространстве. Только так можно обеспечить безопасность и стабильность нашего общества в эпоху информационных технологий» [25, с. 13].

Для обеспечения национальной безопасности необходимо принимать меры по борьбе с информационным терроризмом, включая обучение населения критическому мышлению, укрепление кибербезопасности и сотрудничество на международном уровне.

И наконец, существуют угрозы информационной безопасности личности как составной части безопасности государства. «Правовой статус человека зависит от сущности социального строя, в условиях которого он формируется и функционирует, поэтому становление информационного общества обуславливает необходимость юридического закрепления и государственного гарантирования правового статуса человека на новом качественном уровне. В информационных общественных отношениях человек может брать участие и как субъект (например, отношения по доступу к информации, право на приватность и т. п), может быть их объектом

(отношения по информационной безопасности), а даже – средством (отношения по манипуляции сознанием). Рядом с информатизацией в вышеизложенном «положительном» понимании происходит соответствующий негативный социальный процесс» [2, с. 316].

«Конституции большинства демократических (и не только) государств определяют приоритетность человека, как основной социальной ценности. А обеспечение его прав и свобод – основная задача. В современном мире проблема прав человека вышла далеко за пределы отдельного государства, а объем прав и свобод человека в современном обществе определяется не только особенностями определенного сообщества людей – национального государства, но и развитием человеческой цивилизации в целом» [3, с. 354].

«Поскольку, процессу развития идеи прав человека свойственны как количественные, так и качественные изменения, то, бесспорно, стоит согласиться с расширяющим мнением о коллективном праве человека (третье поколение), возвышении и углублении права на информационное пространство мира, на предоставление различных услуг, которые основываются на интеллектуальных информационных технологиях (в частности на новейших технологиях исследований) и технологиях связи (глобальная сеть «Интернет»), обеспечение информационных отношений» [4, с. 52].

В условиях динамично развивающейся информационной среды, характеризующейся небывалым уровнем цифровизации и глобального информационного обмена, правовое регулирование информационных прав человека обретает особое значение. Невозможно рассматривать информационные права человека в отрыве от контекста функционирования общества и государства, поскольку информационное влияние, оказывая воздействие на общественные процессы и государственную политику, опосредованно затрагивает интересы каждого индивида.

Следует отметить, что личность человека является как исходной предпосылкой, так и конечным результатом развития общества и государства.

Современный человек, будучи неотъемлемой частью информационной реальности, подвергается постоянному воздействию информации, распространяемой как целенаправленно, так и в силу объективных обстоятельств. Понятие "пространство" в контексте информационных процессов приобретает новое, расширенное значение, охватывая не только традиционные физические среды, такие как атмосфера, стратосфера, космос, а также водные акватории океанов и морей, но и современные кибернетические и виртуальные системы. В связи с этим, «актуальным становится вопрос о правовом статусе лица в информационном обществе и государстве, который должен быть подкреплен четко определенным и достаточным объемом информационных прав человека. В современных научных исследованиях, посвященных проблематике информационных прав человека, отсутствует единый, общепризнанный подход к их определению и правовому регулированию.

На основании вышеизложенного можно сделать вывод, что в основе информационной безопасности личности лежит право на свободу в информационной сфере и на предупреждение угроз информации, циркулирующей в технических системах (защита психики и сознания). Совершенствование законодательства об информационной безопасности граждан, прежде всего должно быть связано с защитой персональных данных» [14, с. 14].

«В условиях роста цифровой информатизации, а также перехода экономики в электронное пространство, правонарушитель может завладеть личными данными любого гражданина и воспользоваться ими в любой месте нашей страны или даже за рубежом. Поэтому очень важно на сегодняшний день установить доверие граждан к государственным органам по защите персональных данных. Любой гражданин, совершающий покупки в интернете, либо общающийся в социальных сетях, находится под угрозой и может стать потенциальной жертвой неправомерного завладения конфиденциальных данных. Зачастую для получения услуги в Интернет –

пространстве необходимо сообщать личные сведения о себе: фамилия имя и отчество, возраст, паспортные данные, счет кредитной карты, и другие данные» [31, с. 93].

«Незаконным по действующему законодательству является ведение баз с данными о клиентах. При этом закон «О персональных данных» разрешает гражданину давать согласие на обработку своих персональных данных свободно по своему усмотрению. Юридические лица обрабатывающие персональные данные гражданина зачастую нарушают закон и сохраняют личные данные своих клиентов, вне зависимости от того давали ли они свое согласие на использование их персональных данных или нет. В дальнейшем они могут использовать персональные данные граждан, например в рекламных целях. По действующему законодательству все персональные данные необходимо удалять сразу же после их обработки. Накопление персональных данных, а тем более их дальнейшая продажа или покупка, строго запрещены законодательством» [34, с. 228].

Для реализации и совершенствования обеспечения информационной безопасности граждан в России необходима также сплоченная работа федеральных, региональных и местных государственных органов по повышению уровня информационной безопасности в государстве; совершенствование информационной инфраструктуры посредством обмена международного опыта; повышение эффективности информационной системы прогнозирования, выявления и совершенствование методов борьбы с угрозами информационной безопасности; разработка новых и совершенствование действующего законодательства в сфере защиты информации; усиление юридической ответственности за нарушение законодательства по защите информации; постоянное совершенствование государственной информационной политики в сфере информационной безопасности.

2.2 Правовое противодействие современным вызовам и угрозам информационной безопасности

Программой развития цифровой экономики России, утвержденной постановлением Правительства Российской Федерации «О системе управления реализацией программы «Цифровая экономика Российской Федерации» от 28.08.2017 года № 1030, были обозначены приоритетные направления цифровой экономики, в том числе связанные с обеспечением информационной инфраструктуры и ее безопасного функционирования.

Согласно ч. 4 ст. 6 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» обладатель информации обязан принимать меры по ее защите [38]. К числу таких мер относятся правовые, организационные и технические. Их целью является:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализация права на доступ к информации (ч. 1 ст. 16 Закона об информации).

Обладателями подлежащей защите информации являются организации и физические лица, Российская Федерация, субъект РФ, муниципальное образование (ч. 1 ст. 6 Закона об информации).

«Цели, связанные с обеспечением информационной безопасности, находятся в области защиты информационных данных и поддерживающей цифровой инфраструктуры от преднамеренных или случайных вмешательств, способных повлечь за собою потерю информационных данных или несанкционированное изменение информации» [9, с. 29].

По сути, информационная безопасность выступает в качестве набора методов управления, стандартов и технологий, необходимых для защиты информационных данных и поддерживающей цифровой инфраструктуры.

«Тенденции развития российского законодательства об информационной безопасности граждан связаны с их защищаемыми законодательством интересами. Конституционный принцип свободы массовой информации (ч. 4 и 5 ст. 29 Конституции РФ) на самом деле имеет пределы своего распространения, касающиеся не только названного в ч. 4 перечня сведений государственной тайны» [12, с. 199].

«Конституционные ограничения права на информацию, предусмотренные частью 3 ст. 17 и частью 3 ст. 55 Конституции РФ, направлены на запрет распространения следующих видов информации:

- разжигающей национальную ненависть и рознь;
- фальсифицированной и нарушающей нормы приличия и нравственности;
- посягающей на честь и достоинство граждан, представляющей опасность и вред физическому и духовно-нравственному состоянию людей;
- искажающей память о прошлом, историю страны, посягающей на отечественные ценности поколений;
- инициирующей разрушительные процессы (техногенные, природные, социальные)» [19, с. 199].

Как в любом демократическом государстве, «в России существуют и специальные ограничители информации - это разного рода запрещенная для посторонних лиц информация. Ограниченность распространения такой информации может быть продиктована интересами государственной безопасности, бизнеса, органов публичной власти.

Действующим законодательством закреплен целый ряд прав граждан на охрану их личной информации (врачебная тайна, тайна исповеди, тайна

усыновления, журналистская тайна, банковская тайна, депутатская тайна, тайна персональных данных и др.)» [8, с. 91].

Вопрос о закрытости (тайне) информации непосредственно связан с интересами граждан даже тогда, когда информация не является личной. Так, сохранение государственной тайны необходимо для обеспечения защиты государственного суверенитета нашего государства, а значит, всего общества и каждого гражданина. Сохранение коммерческой тайны, возможно, не так очевидно для обеспечения интересов каждого отдельного гражданина, но с учетом действия рыночных законов эта норма обеспечивает бизнесу благоприятные условия для конкуренции в производстве товаров и услуг, а значит, дает возможность более полного и качественного удовлетворения потребностей граждан.

Обилие информационных ресурсов и переход с бумажной на интернет-платформу делает этот ресурс с учетом международного характера последней недостаточно управляемым и контролируемым с точки зрения необходимости минимизации его негативного воздействия на защищаемые внутренним законодательством государственные, общественные и личные интересы граждан.

В соответствии с ч. 6 ст. 10 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

«Характер размещаемых противозаконных «иных» сведений довольно разнообразный, но с учетом обширной судебной практики уже можно их систематизировать в следующие группы: информация, направленная на подмену функций органов исполнительной власти, рекламирующая возможность предоставления государственных услуг за плату. Например,

предоставление сведений из ЕГРН с использованием официальной символики Федеральной службы государственной регистрации, кадастра и картографии; информация, посягающая на централизованную систему денежного и валютного регулирования в стране:

- о криптовалюте, представляющей собой виртуальные средства платежа и накопления, не обеспеченные реальной стоимостью, не эмитированные государством, не подконтрольные публичной власти;
- различные сайты с информацией, направленной на обучение "Как грамотно инвестировать в биткойн, блокчейн и криптовалюты";
- о действии платежных систем, позволяющих передавать средства без участия банков Tagilcoin, Bitcoin, Ethereum и другие средства платежа;
- о способах и схемах обналичивания денежных средств» [40, с. 5].

«Информация о реализации товаров и услуг, запрещенных к обороту на территории Российской Федерации, а также информация о деятельности, подлежащей лицензированию, государственному регулированию и контролю:

- о реализации товаров, свободная продажа которых запрещена, в том числе о реализации алкогольной продукции, табачных изделий, этилированного бензина, изделий из драгоценных металлов и камней, агрохимикатов, донорских органов, огнестрельного боевого оружия, лекарственных средств и медицинских изделий без рецептов, продаже устройств, препятствующих видеофиксации государственных регистрационных знаков транспортных средств, особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу РФ и (или) охраняемым международными договорами Российской Федерации;
- о продаже поддельных документов (дипломов об образовании без прохождения обучения, различных медицинских справок без обследования, служебных удостоверений сотрудников правоохранительных органов, водительских удостоверений);

– о предоставлении интимных услуг» [40, с. 6].

Информация о различных способах и методах совершения противоправных деяний, за которые может последовать уголовная и административная ответственность:

– содержащая технологии производства и изготовления взрывчатых веществ и взрывных устройств, способах их применения, схемах камуфляжа взрывного устройства под бытовой предмет;
– о способах уклонения от воинской службы и воинской обязанности, от уплаты налогов;
– о способах изготовления, дозировки и употребления наркотических средств и наркосодержащих веществ;
– о фиктивных браках как способе легализации иностранных граждан на территории государства;

«Информация, способная причинить вред здоровью и развитию несовершеннолетних детей:

– побуждающая детей к самоубийству, агрессии, к употреблению наркотических и психотропных веществ, к азартным играм, проституции, бродяжничеству и попрошайничеству;
– обосновывающая или оправдывающая допустимость насилия и жестокости, противоправное поведение;
– отрицающая семейные ценности, пропагандирующая нетрадиционные семейные отношения, неуважение к родителям и другим членам семьи;
– содержащая нецензурную брань либо информация порнографического характера;
– о незаконной продаже курительных смесей и синтетических стимуляторов» [40].

Информация, которая может быть использована в целях причинения вреда:

– содержащая персональные данные граждан;

– содержащаяся на сайтах-анонимайзерах, позволяющая получить доступ к запрещенным материалам.

«Предполагается, что это не исчерпывающий список и информация, которая есть в Интернете, ежедневно пополняется противозаконными сведениями, что свидетельствует о ее колоссальном объеме и необходимости ежедневного мониторинга и анализа.

На доктринальном уровне уже сформулирован тезис о том, что государство должно обеспечить защищенность граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности. Свое развитие данный тезис нашел в более поздних документах Правительства РФ, где отмечается, что для предотвращения угроз информационной безопасности граждан необходимо с раннего возраста прививать знания по распознаванию фишинговых сайтов и писем, телефонного мошенничества, созданию надежных паролей, распознаванию недостоверной информации и другого вредоносного контента» [12, с. 198].

Реализация государственной политики в сфере информационной безопасности основывается на фундаментальных принципах, направленных на укрепление ответственности государства в информационном пространстве, а также на консолидацию усилий гражданского общества. В контексте консолидации усилий гражданского общества особое значение приобретает активизация информационных кампаний, направленных на повышение осведомленности граждан о вопросах информационной безопасности, а также на формирование ответственного подхода к защите персональных данных в цифровом пространстве. В целях усиления правовой регламентации в области информационной безопасности в апреле 2020 года были внесены существенные изменения в Административный и Уголовный Кодексы Российской Федерации. В частности, были введены новые статьи, устанавливающие ответственность за публичное распространение заведомо ложной информации, способной представлять угрозу жизни и безопасности

граждан. Данная мера обусловлена возрастающей актуальностью борьбы с дезинформацией и манипуляцией в информационном пространстве.

Указанные изменения законодательства представляют собой реакцию на объективные реалии развития информационного общества и направлены на обеспечение правовой основы для защиты от информационных угроз, в том числе путем противодействия распространению недостоверной информации, способной причинить вред жизни и безопасности граждан.

«Внедрение и развитие правовых основ информационной безопасности граждан осуществляется не только на основе конституционных норм и доктринальных положений, но также на базе отраслевых нормативных правовых актов и постановлений высших судебных инстанций Российской Федерации. Именно в данных документах более детально и предметно освещены вопросы информационной безопасности граждан, наряду с общими принципами политики предоставления потребителям публичной информации» [12, с. 199].

Так, проблемным участком в области защиты прав потребителей оказалась сфера рекламного сопровождения предоставления гражданам товаров и услуг, в области санитарно-эпидемиологического благополучия граждан - сфера информационного обеспечения защиты здоровья населения, в области защиты прав детей - сфера защиты от вредной информации [21, с. 57].

«Информационным дефектом в сфере рекламы товаров и услуг, не обеспечивающим или даже угрожающим интересам граждан, является недостоверная и недобросовестная реклама (ст. 5 Федерального закона «О рекламе»), за распространение которой предусмотрена соответствующая юридическая ответственность. Особое внимание необходимо уделять информации, адресатом которой являются дети. Детская психика более чувствительная, чем взрослая, и в большей степени подвержена внешнему влиянию. Требуется обезопасить самих детей, их жизнь и здоровье. Детская бравада и стремление скорее повзрослеть толкают их к употреблению

наркотических и психотропных средств, занятию экстремальными (чаще всего противозаконными) видами деятельности, способствуют отчуждению от семейных традиций и ценностей, превалированию в отношении к окружающим их людям культа силы. Задачи информационной безопасности по отношению к этому контингенту граждан заключаются, наряду с законодательными запретами, и в проведении воспитательных мер, обеспечивающих позитивную социализацию детей, формирование у них механизмов критической оценки получаемых сведений» [32, с. 92].

Своевременное и оперативное предоставление достоверных информационных ресурсов для обеспечения санитарно-эпидемиологического благополучия населения - залог его безопасности и здоровья. Именно здесь высока ответственность государственных структур, от которых зависит жизнь и здоровье жителей целых населенных пунктов и регионов. Массовость и ценность объекта угроз предопределяют важность профилактической работы по мониторингу чрезвычайных ситуаций и своевременного доведения информации об угрозе жизни и здоровью людей для предотвращения негативных последствий. В свою очередь, граждане должны иметь возможность самостоятельно получить от компетентных органов и организаций всю информацию, которая может каким-то образом обеспечить сохранение принадлежащих им ценностей, включая прежде всего их здоровье и жизнь, тем более что в силу ч. 3 ст. 41 Конституции РФ сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, влечет за собой ответственность в соответствии с федеральным законом.

В последнее время стала актуальной проблема сексуального просвещения несовершеннолетних, в связи с чем 5 декабря 2022 г. была внесена новая редакция ст. 6.21 КоАП РФ о запрете пропаганды информации о смене пола, о нетрадиционных сексуальных отношениях и (или) предпочтениях.

«Среди такого рода информационных ресурсов статья 8 Федерального закона «О санитарно-эпидемиологическом благополучии населения» выделяет информацию о состоянии среды обитания, качестве и безопасности продукции производственно-технического назначения, пищевых продуктов, товаров для личных и бытовых нужд, о потенциальной опасности для здоровья человека выполняемых работ и оказываемых услуг» [28, с. 78].

Логичным видятся предложения «о создании механизма мониторинга состояния защищенности личности от внутренних и внешних угроз в информационной сфере, а также учреждения института Уполномоченного по защите прав личности в информационной сфере при Президенте РФ». «Это позволит систематизировать разнообразную государственную и общественную деятельность по выявлению и оценке информационных ресурсов, угрожающих безопасности граждан, институализировать ее организационную основу, придать ей более предметный, целенаправленный характер, консолидировать с другими важными направлениями государственной деятельности» [20, с. 20].

Как в любом ином государстве, «режим информационной гарантированности и безопасности граждан в России непосредственно связан с режимом чрезвычайных ситуаций, которые могут быть вызваны военными действиями, природными катаклизмами, техногенными авариями, эпидемиями, массовыми беспорядками и иными чрезвычайными событиями, повлекшими массовое ухудшение состояния благополучия граждан на определенной территории государства, угрожающими их жизни и здоровью. На этот счет существует целый ряд федеральных актов, предписывающих алгоритм действий каждого уровня представителей публичной власти. Не последнее место среди этих мер отведено вопросам информационного обеспечения, предназначенного для урегулирования этих ситуаций в режиме, который будет максимально способствовать прежде всего интересам самих граждан» [20].

Последние события, связанные с военной операцией России на Украине, актуализировали проблемы информационного противодействия воюющих сторон. Провокационная и сфальсифицированная информация противника, особенно в Интернете, наносит порой не менее тяжелый урон нашим интересам, чем его военные и террористические операции. Неслучайно эту войну называют гибридной, понятие которой связано с тем, что нападающая сторона, не прибегая к прямому вторжению, подавляет своего оппонента, используя сочетание скрытых операций, диверсий, кибервойн.

Принятый еще до начала военной операции на Украине федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации впервые собрал и ранжировал субъекты и объекты информационной инфраструктуры в зависимости от областей их использования (социальной, политической, экономической, экологической, а также с точки зрения оборонной, государственной и общественной безопасности).

Само понятие объекта критической информационной инфраструктуры связано с информационными системами, информационно-телекоммуникационными сетями, автоматизированными системами управления субъектов критической информационной инфраструктуры, а также с управленческими, технологическими, производственными, финансово-экономическими и (или) иными процессами в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры в вышеуказанных областях их использования. Перечень сфер критической информационной инфраструктуры включает в себя: здравоохранение, науку, транспорт, связь, энергетику, банковскую сферу и иные сферы финансового рынка, топливно-энергетический комплекс, области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности (п. 8 ст. 2 Федерального закона «О безопасности

критической информационной инфраструктуры Российской Федерации») [39]. При этом категория (первая — самая высокая, вторая и третья) устанавливается правительственной комиссией по категорированию с учетом показателей значимости объектов критической информационной инфраструктуры, установленных в каждой отраслевой сфере объектов информационной инфраструктуры.

Характерно, что ранжирование этих категорий в каждой области использования (социальной, политической, экономической и т.д.) зависит как от характера причиненного ущерба (угрозы его причинения), так и от степени его распространенности (чем большему количеству людей этот ущерб причинен, тем выше категория). Следует иметь в виду, что владельцами (субъектами) этих информационных ресурсов являются не только государственные органы и учреждения, но и юридические лица, индивидуальные предприниматели, которым на праве собственности, аренды или ином законном основании принадлежат информационные системы и сети. Все эти собственники и владельцы должны сознавать, что в условиях сбоя или повреждения их информационных систем происходит массовое, порой необратимое нарушение прав и свобод граждан, причем в наиболее важных и существенных для жизнеобеспечения сферах.

Острая потребность в высоких компьютерных технологиях и программах, которые используются в современных информационных системах, отсутствие или дефицит соответствующих специалистов в IT-индустрии, массовый отток с отечественного рынка иностранных промышленных продуктов в области создания компьютерных программ, производства интеллектуальных продуктов, изделий и комплектующих, несомненно, негативным образом влияет на уровень информационной безопасности российского государства и наших граждан.

Глава 3 Основные проблемы обеспечения информационной безопасности в РФ

3.1 Уголовно-правовые и криминологические механизмы обеспечения информационной безопасности

Современные компьютерные технологии позволяют не только интенсифицировать любой созидательный общественно-полезный процесс, но и дают в руки преступных элементов также мощные источники подготовки и совершения преступлений. В современных компьютерных системах и системах связи имеются уязвимые места, которые могут быть использованы для получения несанкционированной информации, модифицирования программ или нарушения функционирования важнейших систем. Обнаружение таких противоправных действий является сложной задачей, а идентификация нарушителей становится еще более затрудненной.

Специфической особенностью противоправных действий в кибернетическом пространстве является тот факт, что привлекаемые злоумышленниками средства и ресурсы относительно доступны, а проникновение в информационные системы может осуществляться на операционном, программном, сетевом и аппаратном уровнях, а также можно выделить их растянутость как во времени, так и в пространстве. Благодаря широкому развитию глобальных компьютерных сетей злоумышленник может располагаться за тысячи километров от объекта своих действий, с другой стороны, он может ввести в программу дополнительную команду, которая будет выполнена только при наступлении определенного события или даты. Кроме того, естественно, что подобные виды противоправных действий предполагают определенную подготовку, т.е. навыки владения компьютерной техникой, и практически всегда компьютерные преступления имеют связь с другими некомпьютерными видами преступлений [29, с. 169].

Возрастающая статистика международных компьютерных преступлений и растущая угроза, которую эти преступления представляют для экономической безопасности, вызывают необходимость неотложной унификации законодательства в этой сфере.

В России в настоящее время приняты законодательные акты, призванные нормализовать отношения в области использования информационных технологий, а также накоплен огромный опыт, как по безопасности компьютерных систем, так и по анализу преступлений в этой сфере. Важным шагом к усилению защищенности компьютерной информации стало включение в Уголовный кодекс гл. 28 Особенной части УК, посвященной компьютерным преступлениям, где в ст.ст. 272, 273, 274 законодатель выделил ряд норм, направленных на охрану компьютерной информации. Как известно, российское уголовное законодательство призвано обеспечивать охрану наиболее значимых общественных отношений от преступных посягательств, а именно: «охрана прав и свобод человека и гражданина, собственности, общественного порядка и общественной безопасности, окружающей среды, конституционного строя Российской Федерации от преступных посягательств» (ст. 2 УК). Таким образом, уголовная ответственность за преступления в сфере информационной безопасности предусмотрена рядом статей УК, размещенных в Особенной части Уголовного кодекса РФ. Следовательно, любое преступное посягательство на определенный объект уголовно-правовой охраны затрагивает нарушение информационного составляющего данного объекта.

Нарушения информационной безопасности в большей степени проявляются в случае мошенничества в финансовом секторе, в сфере кредитования, страхования, при получении денежной компенсации путем предоставления заведомо ложных или недостоверных сведений либо путем умолчания о значимых фактах, а также при хищении имущества путем ввода, удаления, блокирования, модификации компьютерной информации. Таким образом, большинство преступных посягательств, объектом которых

являются различные социально-значимые интересы (общественные отношения), нарушают общественные отношения в сфере обеспечения информационной безопасности.

Общеизвестным фактом является то, что использование юридических мер для ограничения компьютерных преступлений может быть недостаточно эффективным. Проблема безопасности компьютерных систем требует комплексного решения. На комплексный подход ориентирует и само понятие «компьютерной системы» – это совокупность аппаратных и программных средств компьютерной техники, программного обеспечения и данных, которые обрабатываются или хранятся в ней, т.е. обеспечение безопасности должно включать в себя целый комплекс мер, относящихся ко всем составляющим этой системы.

С точки зрения теории, безопасность любого компонента компьютерной системы, например аппаратуры, программного обеспечения или данных, складывается из трех обязательных условий: доступности, секретности, целостности. При этом доступность состоит в реальном доступе пользователя к работе с компьютерной системой в любой момент времени, т.е. должны быть исключены любые угрозы прерывания: кражи, уничтожения или повреждения аппаратуры, повреждение или удаление программ и данных. Секретность же заключается в том, что любой компонент системы доступен только законным пользователям.

Таким образом, не допускается возможность несанкционированного доступа и перехват программ и данных, т.е. их считывание любым способом или копирование. Целостность означает возможность внесения изменений в программы и данные только лишь законным пользователям, т.е. должны быть пресечены любые попытки операций корректировки данных, изменения в программах другими лицами [34, с. 228].

Учитывая современные угрозы информационной безопасности, существуют различные способы защиты компьютерной техники от физических воздействий и утечки конфиденциальной информации. Нередко

реализация этих угроз образует состав преступлений, предусмотренных действующим Уголовным кодексом Российской Федерации.

Моделирование угроз является крайне необходимым условием построения эффективной системы обеспечения информационной безопасности. Следовательно, под угрозой информационной безопасности в компьютерных системах мы понимаем совокупность условий, создающих потенциальную или реальную опасность нарушения целостности, доступности, конфиденциальности, обрабатываемой в них информации, нарушения надежности реализации функций компьютерной системы.

Многочисленность защитных программных и аппаратных мер обусловлена, прежде всего, массовым использованием компьютеров, которые не содержат в себе серьезных средств защиты. Принцип открытой архитектуры компьютера позволяет быстро и негласно собрать достаточно мощную производительную машину на основе практически любого персонального компьютера, но в то же время снижается уровень безопасности системы. Любой злоумышленник, каким бы способом посягательств он ни пользовался, в однотипных компьютерных системах чувствует себя вполне уверенно, т.к. ему не приходится тратить время и усилия на освоение новых систем и технологий. К аппаратным методам защиты информации относятся, например, устройства для идентификации личности, системы экранирования аппаратуры, кодовые замки и надежные источники питания. Программные методы защиты, в свою очередь, заботятся о безопасности информации, данных и программ, а также о возможности восстановления информации на персональных компьютерах. При передаче информации используются различные методы и системы криптографического преобразования, обеспечивая, таким образом, ее защиту. Благодаря современным методам шифрования смысл сообщений может быть надежно скрыт [40, с. 4].

Существует множество способов взлома системы, но одна из наиболее популярных – это использование ошибок в программе. Ошибки в

программном обеспечении являются одним из самых распространенных видов угроз безопасности в компьютерных системах. Наличие таких ошибок является объективным фактом, обусловленным тем, что программное обеспечение создается не компьютером, а человеком. Несмотря на то, что при создании программного продукта порядка 50% общего времени расходуется на отладку и тестирование программы, гарантировать отсутствие в программном продукте ошибок невозможно.

Самая совершенная на первый взгляд программа устаревает в течение одного года. Не удивительно, что на любую программу ограничения доступа в компьютерную систему через непродолжительное время создается программа, которая её «обходит» или «взламывает». По оценкам экспертов порядка 80% компьютерных взломов становятся возможными вследствие несовершенства парольной защиты компьютерных систем. Использование разными пользователями «популярных» программ серьезно ухудшает положение с обеспечением безопасности.

Массовое распространение компьютерных вирусов – наглядный тому пример. При изучении вопросов программной защиты информационных ресурсов следует обратить внимание на проблему компьютерных вирусов, представляющих угрозу системной безопасности. В настоящее время разработанные зарубежные и отечественные антивирусные программы обладают различными уровнями определения зараженных программ, их компонентов и возможных вредоносных угроз.

Комплексные меры защиты информации направлены на регламентацию функционирования информационных систем, работы персонала, взаимодействия пользователей с системой. Ограничение доступа к ресурсам компьютерной системы обеспечивается, прежде всего, принятием организационно-технических мер ограничения физического доступа несанкционированных пользователей к помещениям, в которых установлены и функционируют элементы компьютерной системы [4, с. 51].

Эта задача решается путем усиления инженерной защищенности помещений, установки систем охранной сигнализации, видеонаблюдения, устройств защиты рабочего места и т.д. Эти меры касаются ограничения доступа к элементам компьютерной системы как физическим объектам. Таким образом, постоянная смена графиков охраны территорий и помещений, работа с персоналом, регулярное обновление используемых программных и аппаратных средств защиты, проведение профилактических мероприятий технических средств может обеспечить безопасность компьютерных систем, сохранность программ и данных в них.

Важно подчеркнуть, что создание системы обеспечения информационной безопасности не заканчивается внедрением средств и методов защиты информации в технологию функционирования объекта защиты. В процессе эксплуатации системы проводится регулярный контроль ее эффективности, осуществляется доработка системы информационной безопасности, вызванная изменениями состава и характеристик средств защиты информации, а также оперативной обстановки и внешних условий деятельности объекта защиты.

Таким образом, как можно заметить, обеспечение информационной безопасности современных информационно-телекоммуникационных систем осуществляется путем принятия целого комплекса разноплановых мер. В связи с этим современные информационные технологии базируются на концепции использования правовых, специальных аппаратных и программных средств, обеспечивающих защиту информации.

С учетом изложенного можно уверенно утверждать, что созданный сегодня законодателем уголовно-правовой механизм обеспечения информационной безопасности позволяет на должном уровне защитить национальные интересы государства в информационной сфере. На сегодня проблема предупреждения компьютерных преступлений является актуальной не только перед правоохранительными органами, но и активными пользователями интернет-сетей. Основная задача заключается в определении

методов и способов противодействия преступным действиям и внедрения их в практической деятельности для обеспечения информационной безопасности.

3.2 Проблемы обеспечения кибербезопасности в РФ в условиях цифровизации системы государственного управления и реализации политики в области информационной безопасности

На сегодняшний день информационные технологии плотно вошли в жизнь каждого человека. Мобильные гаджеты, сеть Интернет, различные мессенджеры и сайты стали обыденностью и основным средством межличностной и групповой коммуникации между людьми и социальными группами. «В закрытых мессенджерах и скрытых разделах сайтов зачастую можно найти любую информацию, в том числе распространение которой запрещено. Возможность посмотреть запрещенные информационные материалы, направленные на разжигание ненависти и вражды, притягивает миллионы пользователей. Во многих популярных социальных сетях при регистрации пользователь обязан ознакомиться с правилами работы информационной площадки, а также согласиться с запретом на распространение деструктивных материалов и публикацию экстремистского контента. Несмотря на то, что пользователи соглашаются и принимают данные условия, оскорбительное поведение, разжигание ненависти и вражды, создание экстремистских информационных групп продолжает расти» [26, с. 57].

В течение последних десяти-пятнадцати лет язык вражды утвердился в качестве ключевого инструментария экстремистских организаций и их адептов, обретая статус доминирующего средства пропаганды. Характерной чертой текстов, написанных на языке вражды, является акцентирование этнических и национальных различий, актуализация деструктивного нарратива о неполноценности отдельных индивидов посредством

использования лингвистических конструкций с целью маскировки враждебного смысла.

Несмотря на то, что в прежние времена язык вражды был подвержен попыткам маскировки, в настоящее время сторонники экстремистских организаций отказались от усложненных лингвистических формулировок, отдавая предпочтение прямому и откровенному выражению оскорбительных, унижающих, ненавистнических и враждебных высказываний.

«В законодательстве Российской Федерации понятие «язык вражды» отсутствует. Кроме того, указанное понятие даже не употребляется в стратегиях национальной безопасности Российской Федерации. На международном уровне понятие «язык вражды» было закреплено еще в 1997 г. Комитетом министров Совета Европы и носило исключительно рекомендательный характер. В 2015 г. на фоне развития экстремистских настроений, связанных с большим количеством мигрантов в разных странах, Комиссия Совета Европы по борьбе с расизмом приняла новые рекомендации по борьбе с ненавистью и враждой, в которых понятие «язык вражды» представляет собой «оправдание, поощрение или возбуждение диффамации, ненависти или поношение лица или группы лиц, любое притеснение, оскорбление, формирование негативных стереотипов, стигматизация или угрозы в отношении данного лица или группы лиц, а также оправдание всех этих форм самовыражения, определяющих лицо или группу лиц по признаку расы, цвета кожи, языка, религии или убеждений, национальности или этнического происхождения, а равно места происхождения, возраста, инвалидности, пола, гендерной идентичности, сексуальной ориентации и других характеристик или статуса». Указанное понятие содержит в себе перечисление действий, которые в соответствии со ст. 1 Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» относятся к экстремизму» [22, с. 6024].

«С каждым годом уровень экстремистских настроений в обществе растет, а экстремистские группы и каналы в сети Интернет насчитывают все

больше своих сподвижников, что напрямую связано с высоким уровнем значения информации, процесса информатизации и модернизации общества, а также с развитием информационных технологий, что, в свою очередь, порождает новые проблемы в сфере международной и национальной безопасности.

Наиболее остро проблема распространения информации на языке вражды стоит в глобальной сети Интернет, которая не имеет четкого государственного регулирования, а принятие норм о регулировании вызывает высокий уровень порицания со стороны общества. На сегодняшний день экстремистские и террористические организации активно используют язык вражды с целью пропаганды и развития экстремистской идеологии» [24, с. 105].

«В настоящее время уровень агрессии и распространения языка вражды в сети Интернет достиг своего максимума. 24 февраля 2022 г. Президент Российской Федерации выступил с обращением к гражданам Российской Федерации, в котором объявил о проведении специальной военной операции на Украине, чем и воспользовались экстремистские организации, ведущие пропаганду на языке вражды. Большой поток информации в глобальной сети, а также различные IT-технологии и средства поспособствовали развитию и укреплению языка вражды, что привело к росту экстремистских настроений. Кроме того, фейковая информация, публичные призывы к осуществлению экстремистской деятельности, высказывания публичных личностей, содержащие в себе ненависть и вражду к гражданам Российской Федерации, поддержка экстремистских организаций, ксенофобия и национализм со стороны мирового сообщества стали современными вызовами в сфере информационной безопасности Российской Федерации, которые и способствовали становлению нового этапа развития и распространения языка вражды в сети Интернет, противодействие которому будет достаточно долгим и сложным процессом» [33, с. 23].

Успешное противодействие распространению языка вражды в сети Интернет возможно только при условии реализации комплексного подхода, включающего в себя правовые, технические и организационные меры. Необходимо обеспечить тесное взаимодействие всех заинтересованных сторон для эффективного решения данной проблемы.

В этой связи требуется:

- определение понятия «язык вражды» как самостоятельной категории экстремистской деятельности, с установлением четких критериев его идентификации и юридической ответственности за его распространение;
- принятие на федеральном уровне нормативно-правовых актов, направленных на обеспечение информационной безопасности государства и граждан, с акцентом на регулирование распространения информации в сети Интернет и защиту от деструктивного контента;
- разработка и реализация взаимосвязанной программы, направленной на обеспечение национальной и информационной безопасности в сети Интернет, включающей в себя комплекс мер по защите информационного пространства, борьбе с киберугрозами и противодействию распространению языка вражды;
- внедрение в деятельность органов государственной власти современного программного обеспечения, способствующего оперативному мониторингу информации в глобальной сети, в том числе с целью выявления материалов, содержащих язык вражды. Данная мера позволит значительно сократить время реагирования правоохранительных органов, обеспечить эффективность противодействия и повысить уровень информационной безопасности.

Полагаем, что совершенствование правового регулирования по обеспечению защиты информации, обрабатываемой в государственных

информационных системах, в части информационно-технических организационных аспектов, а также телекоммуникационных элементов и программно-аппаратных средств должно проводиться в рамках правового регулирования инфраструктуры информационных технологий. В этом аспекте необходимо регламентировать разграничение ответственности операторов информационных систем, а также лиц, являющихся пользователями таких систем, заявителями в рамках предоставления государственных и муниципальных услуг и иными субъектами, взаимодействующими с органами государственной власти в рамках обмена информацией в электронном виде.

Прежде чем мы рассмотрим сами проблемы обеспечения кибербезопасности и неприкосновенности личных данных в цифровой среде, необходимо определиться, что относится к киберпреступлениям, а это различные типы атак, например, хакерские, фишинговые, вредоносные программы и др. Эти методы используют киберпреступники для незаконного доступа к системам и украденным данным, а также для незаконного доступа к ним. В организации, правительственных учреждениях и индивидуальных пользователях остро стоит проблема киберпреступности. Необходимо предпринять глобальные меры по защите информации и противодействию кибератакам.

«В связи с увеличением объемов и значимости хранения данных, увеличивается риск доступу к личной информации мошенников. Нарушение безопасности и несоблюдение мер защиты может привести к утечке данных, таких как имя, адрес, финансовая информация и иные конфиденциальные данные. Это могло бы иметь серьёзные последствия в отношении индивидуума и организации, в том числе в связи с финансовыми потерями и в связи с угрозами конфиденциальности. Для тех, кто использует цифровые технологии, в приоритете должно быть на первом месте – необходимость защищать – персональные данные.

Недостаточная информированность пользователей об уязвимостях кибербезопасности – одна из основных проблем. Многие не знают, как защитить свои данные. Недостаток грамотности цифрового образования и подготовки к кибербезопасности приводит к тому, что пользователи становятся менее защищенными от киберугроз и киберрисков. Образовательная программа и информационная кампания должны проводиться в целях повышения информированности и подготовки пользователей к мерам безопасности в цифровой среде» [21].

Прежде чем говорить о возможных мерах против мошенников в цифровом поле необходимо определиться какие угрозы и риски могут возникнуть при утечке персональных данных.

Одним из методов обеспечения безопасности в киберпространстве является использование современных технологий защиты данных и криптографии. Это предполагает использование сильных паролей, двухфакторную аутентификацию, шифрование данных в хранилищах и передачу информации. Организациям и пользователям необходимо принимать регулярные меры по обновлению программного обеспечения для устранения уязвимостей и обеспечения безопасности своих систем и данных.

В контексте законодательства об инфраструктуре информационных технологий могут быть предусмотрены также меры юридической ответственности за несоблюдение требований информационной безопасности, порядка взаимодействия субъектов в процессе деятельности по обеспечению информационной безопасности в рамках использования указанной инфраструктуры, а также нарушения требований по защите информации и информационной безопасности.

Определенная корректировка полномочий Правительства РФ и федеральных органов исполнительной власти в сфере регламентации требований по обеспечению информационной безопасности также целесообразна. Однако в целом регулирование требований о защите информации в государственных информационных системах следует оставить

в рамках компетенции ФСТЭК России и ФСБ России в целях обеспечения мониторинга их соблюдения, оперативной корректировки их элементов и функций в соответствии с вновь выявленными угрозами информационной безопасности.

«Информационный терроризм - серьезная проблема, и важно принимать меры для его предотвращения. Пути борьбы с информационным терроризмом:

- образование и осведомленность: обучение людей различным видам информационного терроризма и методам его распознавания поможет им быть более осведомленными и критически мыслящими.
- проверка источников: важно проверять достоверность информации, особенно если она вызывает сильные эмоциональные реакции. Подтверждение информации у надежных источников поможет избежать распространения ложной информации.
- сдерживание дезинформации: активное противодействие дезинформации и ложной информации может включать в себя публичное опровержение, факт-чекинг и обучение навыкам критического мышления.
- сотрудничество: международное сотрудничество в борьбе с информационным терроризмом играет важную роль. Обмен информацией и совместные усилия помогут более эффективно бороться с этой угрозой.
- законодательство: принятие законов и мер по регулированию информационного пространства может помочь в предотвращении распространения террористической пропаганды и кибератак.
- поддержка психологического здоровья: поддержка людей, становившихся жертвами информационного терроризма, включая консультирование и психологическую помощь, также важна» [3, с. 353].

Эффективное противодействие информационному терроризму является неотъемлемой частью обеспечения национальной безопасности и защиты прав граждан. Учитывая трансграничный характер информационных угроз, данная задача требует комплексного подхода, объединяющего усилия государственных органов, гражданского общества и международного сообщества. В рамках национального уровня необходимо разработать и реализовать комплекс мер, направленных на предотвращение, пресечение и минимизацию последствий информационного терроризма.

«Стремительный технологический прогресс, происходящие глобальные и национальные события, рост геополитической напряженности оказывают прямо пропорциональное воздействие на рост объемов и уровня сложности кибератак, изменения методологий, используемых хакерами. Современные технологии позволяют наносить вред критически важным системам различного уровня, обходя традиционные системы обеспечения безопасности, находить уязвимости в программном и аппаратном обеспечении, реализовывая долгосрочные и сложные атаки на государственные органы и предприятия различных сфер деятельности» [25, с. 13].

«На фоне активного изменения ИТ-ландшафта возрастает интенсивность кибератак на промышленные объекты, перерабатывающие предприятия, наблюдается усиление тренда на кибератаки с разрушительными последствия, парализующие отдельные компоненты бизнеса или нацеленные на полную блокировку основной деятельности предприятия. Явный акцент прослеживается на целенаправленные атаки систем государственного управления и объекты критической информационной инфраструктуры» [15, с. 50].

В 2023 году кибернетические атаки стали неотъемлемым элементом функционирования субъектов хозяйствования и некоммерческих организаций во всех сферах экономической деятельности. Анализ статистических данных о кибернетических инцидентах, проведенный в 2023 году, выявил тенденцию,

согласно которой государственные органы власти, а также медицинские и образовательные учреждения подвергаются наиболее интенсивному воздействию кибератак. В частности, государственный сектор в 2023 году по-прежнему лидирует по количеству зафиксированных кибернетических инцидентов.

Следствием кибернетических атак стали существенные нарушения в функционировании государственных учреждений.

Согласно актуальным данным, в 2023 году 11 % от общего количества успешно реализованных кибератак были направлены на объекты здравоохранения. Примечательно, что в 44 % случаев подобных атак наблюдались существенные нарушения в функционировании ключевых видов деятельности и бизнес-процессов, что свидетельствует о значительном ущербе, наносимом киберугрозами. В контексте кибератак на медицинские организации наиболее распространенным типом вредоносного программного обеспечения выступают вирусы-шифровальщики, которые нередко используются для блокирования доступа к критически важным данным.

«Значительный рост кибератак в 2023 году по сравнению с аналогичными показателями 2022 года наблюдался и в организациях сферы науки и образования. В данной отрасли влияние вредоносных программ представлено следующими действиями:

- кража личных данных. Киберпреступники направляют атаки на учреждения образования с целью получения доступа к личным данным для дальнейшего использования в мошеннических целях;
- атаки типа Ransomware (трояны-вымогатели). Хакеры блокируют доступ к системам учебных заведений и требуют выкуп за его восстановление;
- подрыв стабильности функционирования. Кибератаки могут создавать хаос и нарушать нормальное функционирование учебных заведений, вызывая проблемы с обучением и выполнением административных задач;

– тестирование уязвимостей. Некоторые хакеры могут использовать образовательные учреждения для проверки своих навыков и возможностей в области кибератак» [15, с. 51].

В начале приемной кампании 2022 года информационные ресурсы высших учебных заведений Российской Федерации, расположенных в различных регионах страны, подверглись массированной атаке, осуществленной с использованием технологии распределенного отказа в обслуживании (DDoS). Выбор периода активности киберпреступников не носил случайный характер. Их действия, направленные на создание условий, препятствующих доступу к информационным ресурсам вузов в период зачисления абитуриентов, могли повлечь за собой неблагоприятные экономические и социальные последствия. С подобной проблемой столкнулись высшие учебные заведения, расположенные в Нижегородской, Астраханской, Оренбургской, Тюменской, Кемеровской областях, Красноярском крае, Республике Коми, Республике Татарстан, Чеченской Республике, Республике Бурятия и других регионах Российской Федерации.

«На фоне усложнившейся геополитической ситуации резко увеличилась доля кибератак на организации финансового сектора. Помимо утечек персональных данных клиентов и коммерческой информации, привлекательным для киберпреступников является кража финансовых средств. По итогам 2023 года значительно выросла и количество официально подтвержденных киберинцидентов на промышленных предприятиях. В наибольшей степени подвергались атакам предприятия автотранспортной отрасли и логистической сферы, производители микроэлектроники, предприятия металлургической промышленности и тяжелого машиностроения. В частности, в конце ноября 2023 года специалисты по информационной безопасности компании Bi.Zone сообщили о том, что киберпреступная группировка Rare Wolf («Редкий волк») в период с начала 2023 года осуществила 97 атак на российские организации, включая компании из сферы тяжелого машиностроения» [7, с. 89].

«В качестве ключевого типа угроз кибербезопасности специалисты выделяют вредоносное программное обеспечение, используемое в целях нанесения ущерба персональным компьютерам или сетевой ИТ-инфраструктуре посредством неправомерного внесения изменений или удаления файлов, получения конфиденциальных данных, отправки электронных писем вредоносного содержания.

После февраля 2022 года рост кибератак на российскую инфраструктуру значительно увеличился. Государственные учреждения и коммерческие организации стали активнее инвестировать в защиту своих данных. Исследование Центра Стратегических Разработок подтверждает формирование отечественных решений в области кибербезопасности и приоритет защиты информации. Отечественные производители продуктов информационной безопасности в целом высоко оценивают результаты действий правительства по усилению киберзащиты» [7, с. 90].

«Высокий спрос на государственные заказы в области информационной безопасности обусловлен необходимостью обеспечения безопасности и защиты важной информации для государственных структур, что делает этот сегмент рынка востребованным. Соотношение числа государственных заказов, связанных с кибербезопасностью, прежде всего, связано с такими важными критериями, как:

- конфиденциальность и безопасность данных;
- строгие требования и регуляции;
- долгосрочные контракты;
- финансирование;
- адаптивность к изменяющимся угрозам и технологиям;
- международное сотрудничество и обмен информацией;
- внедрение современных технологий и методов защиты» [15, с. 51].

Государство выделяет значительные бюджетные средства на финансирование мер по обеспечению кибербезопасности. В числе приоритетных направлений финансирования выделяются:

– разработка и внедрение унифицированной среды безопасной разработки программного обеспечения. Данное направление требует инвестирования в разработку специализированных инструментов, обучение персонала и поддержку стандартов информационной безопасности, направленных на обеспечение безопасного жизненного цикла программного обеспечения;
– мониторинг фишинговых сайтов и других угроз в информационном пространстве;
– создание и развитие отраслевых центров компетенций в сфере информационной безопасности;
– финансирование технологических центров исследования безопасности ядра Linux.

Указанные направления финансирования свидетельствуют о высоком уровне государственной значимости обеспечения информационной безопасности Российской Федерации.

В условиях текущих тенденций цифровизации и возрастающей востребованности удаленных форматов работы, спрос на решения по обеспечению информационной безопасности сохраняется и, по прогнозам, будет продолжать увеличиваться.

Указанные факторы подчеркивают необходимость дальнейшего финансирования мероприятий по укреплению кибербезопасности, а также активного внедрения соответствующих правовых и технических мер, способствующих снижению рисков и повышению защищенности информационных ресурсов.

Заключение

Подведем итоги и сделаем выводы по работе. Для достижения устойчивого развития правовой политики Российской Федерации в сфере информационной безопасности первостепенным фактором является повышение результативности законотворческой деятельности. Это обусловлено необходимостью оперативного реагирования на динамично изменяющиеся вызовы и угрозы информационной безопасности, требующие адекватного правового регулирования. Появление новых нормативно-правовых актов, отвечающих современным реалиям, позволит эффективно решать актуальные проблемы в сфере информационной безопасности, обеспечивая защиту государственных интересов и прав граждан.

Следует отметить, что информационная политика представляет собой комплексную систему, взаимодействующую с различными сферами общественной жизни. Она включает в себя не только технические аспекты, связанные с информационными технологиями и их влиянием на информационную среду (информатика), но также экономические, юридические и политические аспекты, обеспечивающие устойчивое функционирование информационной сферы.

В частности, правовые аспекты информационной политики охватывают широкий спектр вопросов, таких как право на неприкосновенность частной жизни, защита персональных данных, право интеллектуальной собственности, регулирование цифровых платформ, и др. Эффективное правовое регулирование этих вопросов является неотъемлемой частью обеспечения информационной безопасности и гармоничного развития информационного общества.

В современную эпоху цифровых технологий, электронного правительства и перехода от индустриального и постиндустриального общества к качественно новому информационному обществу, возникают

новые задачи и вызовы. Они касаются населения и государств, мирового сообщества, и, со временем они лишь обостряются. Их изучение и обеспечение реализации непосредственно возлагается на соответствующие органы и должностных лиц конкретных государств, ведь фактически на национальном уровне возможно установление определенных регуляторов, в том числе обязывающего или запрещающего характера в информационной сфере.

Следует подчеркнуть что, например, отношения в глобальной сети Интернет еще не отмечаются наличием унифицированных международно-правовых стандартов обязательного характера, основы регламентации таких отношений государства должны определять, прежде всего, на внутригосударственном уровне, в том числе относительно ответственности за их нарушения, причинение убытков правам и свободам человека в информационной и других сферах национальной безопасности.

В условиях стремительного развития информационного общества, характеризующегося повсеместной цифровизацией, приобретает первостепенную актуальность обеспечение информационной безопасности. Современные организации, осознавая ключевое значение информационной безопасности для своей деятельности, функционируют в контексте ускоренного внедрения цифровых технологий. При этом многие инновационные процессы, лежащие в основе развития организаций, основываются на передовых технологиях, обладающих значительным потенциалом для преобразования экономической деятельности. К таким технологиям относятся, в частности, обработка больших массивов данных, облачные платформы, решения на основе искусственного интеллекта и «Интернета вещей», дополненная реальность и роботизация бизнес-процессов. Применение указанных технологий позволяет организациям оптимизировать свою деятельность, достигая повышения экономической эффективности за счет сокращения затрат и времени на осуществление хозяйственных операций, минимизации необходимости использования

посредников и численности персонала, а также снижения роли человеческого фактора в функционировании организации.

Таким образом, информационная безопасность играет одну из ключевых ролей в обеспечении стабильности и рентабельности предприятия и экономики страны в целом. Угрозы информационной безопасности, такие как утечки данных, кибератаки и прочие нарушения, могут привести к серьезным последствиям. Поэтому внедрение соответствующих мер безопасности помогут своевременно предотвратить возможные угрозы и обеспечить надежную защиту.

В России обеспечение информационной безопасности граждан неразрывно связано с возможностью возникновения чрезвычайных ситуаций, вызванных различными причинами, такими как военные конфликты, стихийные бедствия, аварии, эпидемии и массовые беспорядки. Эти события могут серьезно угрожать жизни и здоровью граждан, а также ухудшить их благополучие на определенной территории страны. Законодательство предписывает определенные шаги, которые должны предпринимать представители власти на всех уровнях в случае чрезвычайных обстоятельств. Особое внимание уделяется вопросам информационной поддержки, направленной на эффективное управление подобными ситуациями с учетом интересов граждан.

Создание механизма наблюдения за степенью защиты личности от внутренних и внешних угроз в информационной сфере и учреждение института Уполномоченного по правам личности в информационной сфере при Президенте РФ представляются логичными предложениями. Это способствует систематизации государственной и общественной работы по выявлению и оценке информационных ресурсов, угрожающих безопасности граждан. Институционализация основ этой работы, придание ей более конкретного и целенаправленного характера, а также объединение с другими важными направлениями деятельности государства станут результатом предложенных мер.

Список используемой литературы и используемых источников

1. Алиева З. И., Хасбулатова З. М. Информационная безопасность как составная часть национальной безопасности российской федерации: конституционно-правовой аспект // Юридический вестник Дагестанского государственного университета. 2022. № 3. С. 39-45

2. Алламурадова М. К. Эволюция угроз в области информационной безопасности: анализ современных тенденций и перспективы защиты / М. К. Алламурадова // Вестник науки. 2024. Т. 4, № 3(72). С. 315-319.

3. Бабкин А. В. Информационные угрозы экономической безопасности в условиях цифровизации / А. В. Бабкин, М. М. Балог // Интеллектуальная инженерная экономика и Индустрия 5.0 (ИНПРОМ-2024) : Сборник трудов X Международной научно-практической конференции. В 2-х томах, Санкт-Петербург, 25–28 апреля 2024 года. – Санкт-Петербург: ПОЛИТЕХ-ПРЕСС, 2024. С. 351-355.

4. Баранников Д.Н., Мартынова А.И. Обеспечение информационной безопасности России в рамках реализации Концепции внешней политики // Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика». 2024. № 1. С. 51–64

5. Блинкова А. Е. Информационный терроризм как угроза национальной безопасности / А. Е. Блинкова, М. Ю. Чеснокова // Научный дебют 2024 : сборник статей V Международного научно-исследовательского конкурса, Пенза, 25 февраля 2024 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. С. 42-45.

6. Бочарников И.В. Приоритетные направления информационно-аналитического обеспечения специальной военной операции // Вестник Академии военных наук. 2022. № 4. С. 46 - 53.

7. Бушуев А.Л., Деревцова И.В., Мальцева Ю.А., Терентьева В. Д. Роль информационной безопасности в условиях цифровой экономики //

Baikal Research Journal. 2020. № 1. С. 88-91.

8. Волкова О. Н. Сущность понятия и классификация угроз информационной безопасности / О. Н. Волкова, А. А. Садакова // Образование в цифровую эпоху: опыт, проблемы и перспективы, Нижний Новгород, 21–22 декабря 2023 года. – Нижний Новгород: Нижегородский государственный педагогический университет им. К. Минина, 2024. С. 90-94.

9. Газизов Н. Ю. Информационная безопасность: виды угроз и способы борьбы с ними / Н. Ю. Газизов // Студенческий вестник. 2024. № 1-9(287). С. 29-31.

10. Гринев Н. Н. Цифровизация и угрозы информационной безопасности / Н. Н. Гринев, Т. Н. Шушунова, Н. Ю. Николаева // Транспортное дело России. 2024. № 2. С. 13-15.

11. Дмитриев В. В. Информационные угрозы и вызовы интересам и безопасности России в условиях современной трансформации мирового порядка / В. В. Дмитриев // Информационная аналитика и информационно-аналитические технологии в контексте социального управления, МГТУ имени Н.Э. Баумана, 15 ноября 2023 года. – М. : Общество с ограниченной ответственностью «Издательство «Экон-Информ», 2024. С. 57-73.

12. Дубень А.К. Совершенствование системы информационной безопасности: сравнительно-правовой анализ // Правовая политика и правовая жизнь. 2022. № 2. С. 198-203.

13. Зиновьева Е.С. Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества: монография. - М.: МГИМО-университет, 2021. 280 с.

14. Кожевина О.В. Национальные правовые режимы России и Франции в сфере цифровой безопасности: компаративный анализ // Право и цифровая экономика. 2020. № 2. С. 12 – 16.

15. Куренкова Е. Р. Актуальные угрозы в области информационной безопасности и способы их предотвращения / Е. Р. Куренкова // Студенческие исследования, идеи и инновации : сборник статей II Международной научно-

практической конференции, Пенза, 20 июня 2024 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2024. С. 50-52.

16. Логинова Т.Д. Обеспечение права личности на информационную безопасность (теоретико-правовой аспект): дис. ... канд. юрид. наук. Барнаул, 2019. 138 с.

17. Лопаева А. С. Информационная безопасность в свете развития цифровой экономики в Российской Федерации // Междисциплинарные исследования: опыт прошлого, возможности настоящего, стратегии будущего. 2021. № 1. С. 16-19.

18. Мартынова А. И. Безопасность в сфере информационных технологий: основные угрозы и способы их предотвращения / А. И. Мартынова // Информационные технологии и системы: управление, экономика, транспорт, право. 2024. № 2(50). С. 20-24.

19. Международная информационная безопасность: подходы России. Аналитический доклад / отв. ред. А.В. Крутских, Е.С. Зиновьева. М.: МГИМО, НАМИБ, 2021. 48 с.

20. Михаленко Н.А. Родь информационной безопасности в системе национальной безопасности современной России // Актуальные проблемы правоведения. 2024. № 1 (81). С.19-22.

21. Мандзюк С. А. Вызовы и угрозы информационной безопасности личности в цифровой среде / С. А. Мандзюк, О. А. Егерева // Бизнес и общество. 2024. № 1(41). С. 55-59.

22. Наговицына Т. К. Угрозы информационной безопасности в органах государственной власти / Т. К. Наговицына // Научный аспект. 2024. Т. 47, № 6. С. 6023-6030.

23. Овчинников А.И. Безопасность личности и государства в цифровую эпоху: политико-правовой аспект // Журнал российского права. 2020. № 6. С. 6-12.

24. Перевертун Д.Р. Угрозы информационной безопасности: всесторонний анализ//Международный журнал информационных технологий

и энергоэффективности. 2024. Т. 9. № 5(43). С. 104–108.

25. Поначугин А.В., Грачева Е.А. Проблемы кибербезопасности в современном мире // Дневник науки. 2020. № 10 (46). С. 12-18.

26. Пузырева Ю.В. Актуальные проблемы международно-правового регулирования использования информационных технологий и информационного пространства в современных вооруженных конфликтах // Российский ежегодник международного права. 2023. Т. 2022. С. 56–70.

27. Романова Д. С. Роль информационных технологий в обеспечении национальной безопасности / Д.С. Романова // Научные горизонты. 2020. № 1 (29). С. 181-187.

28. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии: монография / Национальный исследовательский институт мировой экономики и международных отношений имени Е.М. Примакова Российской академии наук. - М.: ИМЭМО РАН, 2020. 97 с

29. Рожкова А. К. Информационная безопасность, угрозы и риски в эпоху постиндустриального общества / А. К. Рожкова // Философия в XXI веке: направления и тенденции развития : Материалы II Международной научно-практической конференции: В 3-х частях, Москва, Зеленоград - Красноярск, 12 апреля 2024 года. – М. : федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Московский институт электронной техники», 2024. С. 169-177.

30. Русанов М. А. Базовая классификация угроз информационной безопасности и методы противодействия им / М. А. Русанов, М. Г. Бабенко // Современное программное обеспечение систем информационной безопасности и интеллектуальной поддержки управленческих решений : Сборник научных статей аспирантов. – М. : Московский финансово-юридический университет МФЮА, 2024. С. 16-20.

31. Сидорова Е.З., Усов Е.Г. Уголовная политика в сфере обеспечения

цифровой безопасности // Вестник Пермского института Федеральной службы исполнения наказаний. 2024. № 2(53). С. 92–99.

32. Соколов А. Ю., Лакаев О. А. Правоохранительная политика в сфере обеспечения информационной безопасности как часть современной правовой политики Российской Федерации: основные тенденции развития //Правовая политика и правовая жизнь. 2021. № 2. С. 91–101.

33. Соколов А. Ю. Правовое противодействие современным вызовам и угрозам информационной безопасности / А. Ю. Соколов // Правовая политика и правовая жизнь. 2024. № 1. С. 22-30.

34. Терещенко Л.К., Зырянов С.М. Правовая модель информационной безопасности в Российской Федерации: структура и ключевые параметры // Вестник Московского университета МВД России. 2019. № 5. С. 227-232.

35. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. – URL: https://www.consultant.ru/document/cons_doc_LAW_208191/ (Режим доступа: 22.09.2024).

36. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», 12.12.2016, № 50, ст. 7074 // «Собрание законодательства РФ», 05.07.2021, № 27 (часть II), ст. 5351.

37. Фарвазова Ю. Р. Совершенствование информационной безопасности как части антитеррористической стратегии России // Вестник Казанского юридического института МВД России. 2014. № 1 (15). С. 115-120.

38. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 08.08.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.10.2024) // «Российская газета», № 165, 29.07.2006.

39. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // «Российская газета», № 146, 03.07.2014.

40. Чемоданова Ю.В. Современные угрозы информационной безопасности РФ // Сибирский экономический журнал. 2019. № 3 (11). С. 4-9.