МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Департамент публичного права
(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 Э.Д. Андроников _____
(Инициалы Фамилия) (личная подпись)

Руководитель канд. юрид. наук, доцент А.А. Иванов
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

Аннотация

Актуальность выпускной квалификационной работы обуславливается тем, что в условиях социально-экономических трансформации общества в XXI в. наблюдается интенсивное проникновение информационно-коммуникационных технологий во все сферы общественной жизни.

В современном глобализированном мировом пространстве вопросы обеспечения информационной безопасности приобретают новые очертания.

Цель исследования – изучение правовой политики в сфере обеспечения информационной безопасности.

Задачи исследования заключаются в рассмотрении теоретических и методологических основ информационной безопасности, освещении вопросов, связанных с гарантиями обеспечения информационной безопасности, выявлении проблем и перспектив развития информационной безопасности.

Структура выпускной квалификационной работы соответствует поставленным целям и задачам и состоит из введения, трех глав, разделенных на параграфы, заключения, списка используемой литературы и используемых источников.

Оглавление

Введение

Актуальность темы выпускной квалификационной работы обусловливается тем, что в условиях социально-экономических трансформаций общества в XXI в. наблюдается интенсивное проникновение информационно-коммуникационных технологий во все сферы общественной жизни.

В современном глобализированном мировом пространстве вопросы обеспечения информационной безопасности приобретают новые очертания. Вопрос о роли и значимости обеспечения информационной безопасности выступает предметом широкого обсуждения в научно-экспертном сообществе.

Однако принимая во внимание масштабы проникновения информационных технологий во все сферы общественной жизни, а также проблему технологической привязанности, на повестку дня поставлен вопрос выработки перспективных направлений обеспечения информационной безопасности.

Кроме того, данная проблема усугубляется на фоне усиления новых вызовов и угроз сохранности информационных систем, которая приобретает особую актуальность не только с точки зрения обеспечения безопасности персональных данных, но и информационного обеспечения органов государственного и муниципального управления.

Объектом исследования выступают общественные отношения, складывающиеся в сфере обеспечения информационной безопасности.

Предметом исследования является совокупность правовых норм, применяемых в процессе реализации правовой политики в сфере обеспечения информационной безопасности.

В качестве цели выпускной квалификационной работы заявлено изучение правовой политики в сфере обеспечения информационной безопасности.

Поставленная в настоящей работе цель определяет необходимость решения следующих задач:

- изучить историю правовой политики в сфере обеспечения информационной безопасности;
- рассмотреть информационную безопасность в структуре национальной безопасности;
- раскрыть общие гарантии информационной безопасности;
- рассмотреть организационные гарантии информационной безопасности;
- изучить нормативные гарантии информационной безопасности;
- выявить проблемы обеспечения информационной безопасности;
- представить перспективы и предложения в области обеспечения информационной безопасности.

В первой главе выпускной квалификационной работы рассмотрены теоретические и методологические основы правовой политики в области обеспечения информационной безопасности: история правовой политики в области обеспечения информационной безопасности; информационная безопасность в структуре национальной безопасности.

Во второй главе выпускной квалификационной работы освещены вопросы, связанные с гарантиями обеспечения информационной безопасности: общие гарантии информационной безопасности; организационные гарантии информационной безопасности; нормативные гарантии информационной безопасности.

Третья глава выпускной квалификационной работы посвящена выявлению проблем и перспектив развития обеспечения информационной безопасности.

Теоретическую основу исследования составили труды отечественных авторов: А.К. Жаровой, Ю.Н. Загинайлова, Р.С. Зариповой, И.Р. Инарокова, П.А. Махмадова, В.С. Остапенко, П.А. Столбова, З.Ю. Точиевой и многих других.

Нормативная база исследования представлена в виде положений законодательства Российской Федерации, регулирующих совокупность общественных отношений, складывающихся в процессе реализации правовой политики в сфере обеспечения информационной безопасности.

Специфика заявленной в выпускной квалификационной работе цели и задач предполагает выбор в пользу комплекса общенаучных методов познания, применяются также и некоторые методы, свойственные частным наукам. При написании выпускной квалификационной работы, в частности, использовались такие методы, как синтез, анализ, а также сравнительно-правовой метод.

Структура выпускной квалификационной работы представлена введением, тремя основными разделами, разделенными на параграфы, заключением и списком используемой литературы и используемых источников.

Глава 1 Теоретические и методологические основы правовой политики в области обеспечения информационной безопасности

1.1 История правовой политики в области обеспечения информационной безопасности

Раскрытие содержания данного параграфа следует предварить высказыванием о том, что технологические и социально-экономические трансформационные процессы XXI столетия привели к смене парадигмы в информационной среде.

Развитие информационно-технологического пространства задает новый вектор развития. Однако не стоит упускать из поля зрения, что вопрос усиления и появления новых вызовов и угроз в новом информационном поле приобретает совершенно иные очертания.

Приступая к исследованию поставленной в данном параграфе задачи, следует определиться с понятийно-терминологическим аппаратом изучаемого предмета на основе дедуктивного и индуктивного методов исследования.

Этимологическое толкование термина «информационная безопасность» – «Information Security» – состояние защищенности информации [28, с. 12].

Вопрос, связанный с определением термина «информационная безопасность», выступает предметом широкого обсуждения в научно-экспертном сообществе. Дискуссионность ему придает отсутствие единого понимания среди представителей науки.

Так, в подходе П.А. Махмадова при его интерпретации автором просматривается смешение данной категории с терминами «устойчивость» и «стабильность» [34, с. 10].

Впрочем, данный подход разделяют не все ученые, вкладывая в его понимание совершенно иной смысл.

Так, в понимании А.В. Зенкова информационная безопасность предстает как многогранная категория, которая с одной стороны воплощает в себе тезис

о защищенности информации от неправомерного доступа, преобразования и уничтожения, с другой как защищенности информации от внешнего воздействия [17, с. 8].

В видении других ученых информационную безопасность, которая выступает неотъемлемой составляющей национальной безопасности [3, с. 259], следует рассматривать как состояние защищенности публичного и частного интересов [5, с. 15] от процессов, связанных с утечкой закрытых сведений; от внешнего и информационного воздействия на индивидуальное и общественное сознание [41, с. 196].

Третьи ученые в данном вопросе руководствуются узким и широким толкованием [11, с. 38]. В их понимании информационную безопасность в узком смысле следует рассматривать как состояние защиты информации от внешнего воздействия [48, с. 31]. В широком смысле – как состояние защищенности национальных интересов [57, с. 31] в интенсивно развивающемся информационном пространстве [64, с. 72].

Группа четвертых ученых при интерпретации термина «информационная безопасность» руководствуется многогранным подходом, определяя его как защищенность информации от преднамеренного вредоносного воздействия, которое наносит неизгладимый урон субъектам информационных правовых отношений [27, с. 37].

Другие ученые в вопросе понимания термина «информационная безопасность» руководствуются его содержательной составляющей, позиционируя данный термин как комплексную систему, целевая направленность которой – защита объектов информационной безопасности от широкого спектра внешних угроз (несанкционированного воздействия) с применением аппаратных и технических решений, информационно-правовых средств [74, с. 212].

И, наконец, в видении шестых ученых информационную безопасность следует рассматривать как совокупность методов [11, с. 50], целевое предназначение которых фокусируется на защите данных от

несанкционированного воздействия на объекты информационной безопасности [75, с. 72].

По мнению автора выпускной квалификационной работы, возрастание научного интереса к категории информационной безопасности обуславливается её провозглашением российским законодателем как составляющей национальной безопасности.

В рамках правового поля определение дефиниции «информационная безопасность» сформировано в Доктрине информационной безопасности Российской Федерации, утвержденной указом Президента РФ от 05.12.2016 № 646 (далее по тексту – Доктрина информационной безопасности, Доктрина ИБ) [60].

Буквальное толкование п. «в» ч. 2 позволяет сделать вывод о том, что информационная безопасность – это состояние защищенности национальных интересов от внешних угроз в информационной сфере, определяющихся совокупностью сбалансированных интересов отдельной личности, общества и государства в целом, а также обеспечения конституционных прав.

Таким образом, теоретическое осмысление проблемы определения термина «информационная безопасность» позволило сделать вывод о том, что в доктрине права не сложилось единого подхода к определению данного термина.

Впрочем, несмотря на расхождение взглядов ученых в понимании данного термина нельзя отрицать, что в проанализированных выше подходах просматриваются общие черты. Здесь стоит обратить внимание на том, что при толковании информационной безопасности представители научного сообщества склоняются к тому, что она является неотъемлемой составляющей национальной безопасности. Определение данного термина в указанном ключе отражает современные реалии – усиление геополитической напряженности, развернутой против Российской Федерации войны в информационной пространстве.

Логика данного параграфа предполагает проведение сравнительного исследования поставленного в нем вопроса сквозь призму исторической эпохи. Исследование данного вопроса на основе исторического сопоставления позволит провести грань между конкретным историческим периодом и настоящим временем.

Становление и развитие информационной безопасности связывается с периодом развития древнерусского государства. В рассматриваемый исторический период обеспечение информационной безопасности осуществлялось на основе сочетания контрольной и других форм деятельности. В частности, для защиты информации от посягательств третьих лиц применялись методы и приемы стенографии и шифрования [40, с. 40].

С момента формирования системы информационной безопасности в Древней Руси и вплоть до начала дореволюционного периода законодатель не придавал вопросам обеспечения информационной безопасности особого правового значения.

Однако в дореформенный период наблюдается усиление военной мощи российского государства и повышение его роли на международной арене, что обуславливало необходимость проведения широкомасштабных реформ, направленных на укрепление информационного суверенитета страны.

Помимо курса государства на обеспечение информационной безопасности в целом Петр I уделял внимание и вопросам сохранения государственной тайны во всех сферах деятельности государственного аппарата. Так, в январе 1724 г. им издан указ «О делах тайности подлежащих», регламентирующий защиту государственной тайны [55, с. 438].

Николай I в определенной степени перенял курс Петра I, что выразилось во введении ответственности за разглашение сведений, составляющих коммерческую тайну.

Однако в целом в Российской империи, согласно высказыванию представителей доктрины права, не сложилось полноценной правовой базы,

механизмов и принципов реализации информационной безопасности [73, с. 134].

На подступах революционных движений вектор развития информационной безопасности сместился в сторону защиты государственной тайны.

Учитывая кризисные тенденции, всколыхнувшие всё гражданское общество, в 1921 году создается Всероссийская чрезвычайная комиссия по борьбе с контрреволюцией и саботажем при Совете народных комиссаров РСФСР, спектр задач которой фокусировался, в том числе, на защите государственной тайны [22, с. 28].

Итак, стоит отметить, что с момента воплощения в законодательных актах идеи информационной безопасности до революционных событий, произошедших в 1917 году, внимание со стороны законодателя её обеспечению заметно возросло.

Разумеется, революционные события, захлестнувшие всю страну, внесли соответствующие коррективы в социально-политическую жизнь общества и отечественное правовое поле. И в данном свете изменения не обошли стороной и вопрос обеспечения информационной безопасности.

Советский законодатель уделял особое внимание обеспечению информационной безопасности, предусмотрев специальные каналы связи для передачи секретных сведений. В 1930-х гг. интенсивно формируется законодательная база, которая по мере развития и укрепления государственности дополнительным образом расширяется и дополняется, получает новые механизмы своей реализации и защиты.

В 1940-х гг. появляются первые шифровальные машины. Однако на фоне их появления наблюдается всплеск недобросовестной деятельности в данном направлении – разработка методов их взлома [12, с. 458].

С 1980-х годов происходит эволюционирование кибернетических угроз, что вызвано широким проникновением в жизнь общества персональных компьютеров и объединяющих их локальных сетей [7, с. 27].

Это ознаменовало новый этап обеспечения информационной безопасности, выразившийся в принятии широкого ряда нормативных правовых актов, в том числе:

– Закона Российской Федерации от 05.03.1992 № 2446-1 «О безопасности» (утратил силу) [15];
– Федерального закона от 20.12.1995 № 24-ФЗ «Об информации, информатизации и защите информатизации» (утратил силу) [66];
– Указа Президента Российской Федерации от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне» [58].

Параллельно развитию законодательной базы в данной области создаются специальные органы защиты информационной безопасности.

В частности, следует отметить учреждение в 1992 году Государственной технической комиссии при Президенте Российской Федерации, спектр деятельности которой охватывал регулирование вопросов информационной сохранности, разработки нормативных актов в данной области.

На рубеже XX – XXI столетий развитие беспроводных сетей с одной стороны открыло новые возможности для государства и общества, а с другой – «вооружило» киберпреступников новыми методами и приемами.

Однако вслед на новые угрозы и вызовы последовала реакция со стороны частных структур: создание организации, специализирующейся на разработке систем защиты от угроз информационной безопасности – АО «Лаборатория Касперского», что позволило укрепить информационный суверенитет Российской Федерации [33, с. 672].

С 2000-хх гг. в Российской Федерации в сфере обеспечения информационной безопасности начинает формироваться правовая база с учетом информационно-коммуникационных трансформаций:

– Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» (устанавливает правовые основы деятельности в области связи) [67];

– Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (регламентирует основные права и коррелирующие им обязанности субъектов общественных отношений в сфере обеспечения информационной безопасности) [68];
– Федеральный закон» от 27.07.2006 № 152-ФЗ «О персональных данных» (определяет основные требования, предъявляемые к «взаимодействию» с персональными данными) [69];
– Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (регулирует отношения в области использования электронных подписей) [71];
– Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (закрепляет положения о защите IT-инфраструктуры) [72];
– Указ Президента РФ от 22.02.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» [59];
– Доктрина информационной безопасности.

Отдельное внимание следует сосредоточить на Доктрине информационной безопасности, содержание которой представлено следующим образом: I. «Общие положения»; II. «Национальные интересы в информационной сфере»; III. «Основные информационные угрозы и состояние информационной безопасности»; IV. «Стратегические цели и основные направления обеспечения информационной безопасности»; V.«Организационные основы обеспечения информационной безопасности».

Также следует отметить и то, что в Доктрине информационной безопасности находит закрепление понятийно-терминологического аппарата в области информационной безопасности:

– информационная инфраструктура Российской Федерации – совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации;
– национальные интересы Российской Федерации в информационной сфере – объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;
– обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;
– силы обеспечения информационной безопасности – государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;
– система обеспечения информационной безопасности – совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

– средства обеспечения информационной безопасности – правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;
– угроза информационной безопасности – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам и информационной сфере.

Таким образом, учитывая масштаб проникновения информационно-коммуникационных технологий в жизнь современного общества, органов государственной власти и экономических субъектов, а также высокий уровень зависимости создаваемых в Российской Федерации информационных систем от импортозамещения, на повестку дня поставлен вопрос обеспечения информационной безопасности страны в условиях новых вызовов и угроз.

1.2 Информационная безопасность в структуре национальной безопасности

В соответствии с Указом Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» (далее по тексту – Стратегия) национальная безопасность Российской Федерации определяется как состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечивается реализация конституционных прав и свобод граждан, достойное качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны [64].

Принятие новой Стратегии обуславливается несколькими причинами: обострение геополитической напряженности; возрастающее за последние несколько лет санкционное давление со стороны недружественных стран. Кроме того, нельзя не отметить, что её разработка обусловлена концепцией

информационного общества и повышением роли информации и интеграции Российской Федерации в глобальное информационное пространство.

В Стратегии обозначены приоритетные направления и задачи, проводимой государством политики в области обеспечения национальной безопасности и составляющей её информационной безопасности.

В рамках представленной Стратегии отмечено, что «последовательно проводимый Российской Федерацией курс на укрепление обороноспособности, внутреннего единства и политической стабильности, на модернизацию экономики и развитие промышленного потенциала обеспечил укрепление суверенной государственности России как страны, способной проводить самостоятельную внешнюю и внутреннюю политику, эффективно противостоять попыткам внешнего давления».

Кроме того, в представленной Стратегии подчеркивается, что «использование в Российской Федерации иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российских информационных ресурсов, включая объекты критической информационной инфраструктуры Российской Федерации, к воздействию из-за рубежа».

Национальная безопасность как многогранная категория с содержательной стороны представлена обороной страны и видами безопасности, предусмотренными Конституцией Российской Федерации, принятой 12.12.1993 г. и законодательством Российской Федерации.

Национальные интересы государства и общества выступают фундаментальной основой информационной безопасности.

При этом на страницах юридической публицистики приводится мысль о том, что уровень развития системы информационной безопасности служит детерминантной развития национальной безопасности страны [3, с. 260]. Данное высказывание не вызывает сомнения, учитывая становление информационного общества, интенсивное развитие информационно-

коммуникационных технологий, порождающих за собой возникновение новых вызов и угроз для национальной безопасности государства.

На этом фоне нельзя оставить без внимания появление новых видов преступлений, которые наносят неизгладимый вред целостности всего информационного пространства страны.

В числе преступлений стоит выделить кибернетический терроризм, кибернетический экстремизм, преступления экономической направленности, которые совершаются с использованием информационно-коммуникационных технологий [2, с. 13].

На современном этапе развития в условиях геополитической напряженности число угроз национальным интересам возрастает. Крайне чувствительной и острой выступает проблема широкого проникновения во все сферы общественной жизни кибернетического терроризма и экстремизма, которые представляют серьёзную угрозу для национальной безопасности.

В указанном ключе заслуживает внимания позиция Верховного Суда Российской Федерации, изложенная в Постановлении Пленума от 15.12.2022 № 37, в котором приводится разъяснение судебной практике по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», в том числе о месте совершения преступления указанных преступлений [44].

Преступления в сфере компьютерной информации следует рассматривать как преступления, причиняющие ущерб интереса отдельной личности [45, с. 152], общества и государства в целом в информационной сфере [10, с. 67].

Исходя из сложившейся правоприменительной практики, стоит отметить, что подавляющее большинство лиц, совершающих преступления в сфере информационных технологий, – это представители мужского пола [48] в возрасте до 30 лет (Приговор Новочебоксарского городского суда Чувашской Республики от 21.12.2016 г. по делу № 1-318/2016; Приговор

Саровского городского суда Нижегородской области от 15.02.2010 г. по делу № 1-14/10) [46].

Помимо того, для большинства лиц, совершающих преступления в сфере информационных технологий, характерно то, что они ранее не судимы (Постановление Лискинского районного суда Воронежской области от 29.07.2020 г. по делу № 1-189/2020 [47]; Приговор Октябрьского городского суда Республики Башкортостан от 29.07.2020 г. по делу № 1-243/2020) [43].

Особое внимание следует обратить на террористические акты во всем их многообразии, которые приобретают глобальный характер, принимая новые очертания в рамках информационно-кибернетического пространства.

К глубокому сожалению, интенсивное проникновение в жизнь современного общества информационно-коммуникационных технологий открывает широкие возможности для недобросовестных лиц.

Таким образом, в настоящее время обеспечение информационной безопасности как составляющей национальной безопасности приобретает особое значение, учитывая интенсивное развитие информационно-коммуникационных технологий, которое порождает возникновение новых вызовов и усиление угроз для национальной безопасности страны.

Последнее десятилетие в особенности обострило проблемы усиления угроз в информационно-кибернетическом пространстве и использования информационных ресурсов для разрушения целостности информационной безопасности государства.

При этом важно учитывать, что истоки данных проблем связываются и с отсутствием законодательной базы в сфере защиты кибернетического пространства, возрастанием напряженности между государствами в кибернетическом пространстве.

Тенденции в данной области сказываются отнюдь не в положительном ключе, и свидетельствуют об уничтожении механизмов, платформ и площадок для ведения диалога и эффективного взаимодействия на высшем уровне по вопросам обеспечения защиты в кибер-пространстве.

В целом, проблемы обеспечения информационной безопасности приобретают особую чувствительность и остроту, требуя объективного и комплексного подхода к их решению.

При этом важно учитывать не только внутренние, но и внешние факторы, новые угрозы и вызовы.

В отдельном освещении также нуждается проблема возрастания угроз в кибернетическом пространстве.

Актуализированные на 2024 год данные свидетельствуют о росте кибернетических атак на 39 процентных пунктов в сравнении с 2023 годом [8].

Тенденция к их возрастанию обуславливается интенсивным проникновением в информационно-кибернетическое пространство вредоносных программ и технологий. В частности, в исследовании И.Г. Александрова приводятся варианты вектора кибернетических атак и иного вредоносного воздействия на информационную безопасность.

Одну из внешних угроз автор ассоциирует с появлением вредоносной программы под названием «Шифровальщик», в результате установки которой на персональный компьютер содержащиеся на нем файлы поддаются вредоносному воздействию.

Не менее серьезную опасность представляет DDoS (Distributed Denial of Service) – сетевая атака, информационное разрушающее воздействие на компьютерные системы посредством направления широкого массива запросов на IP-адрес оборудования пользователя. В результате данного воздействия, как приводится в научном труде И.Г. Александрова, происходит нарушение или полное блокирование обслуживание информационных систем [1, с. 43].

В качестве другой угрозы информационной безопасности автор выделяет кибернетические войны, которые представляют собой противостояние в информационно-кибернетическом пространстве, направленное на дестабилизацию информационных систем, в том числе, государственных информационных систем.

В исследовании Д. Канаева приводится иной взгляд на внешние угрозы в информационно-кибернетическом пространстве. Автор акцентирует внимание на бот-сетях, задачи которых носят широкую направленность, поскольку не ограничиваются рассылкой спам сообщений, но и фокусируются в направлении осуществления DDoS-атак.

При этом недобросовестные лица, создавая бот-сети зачастую преследуют цели оказания вредоносного воздействия, ограничиваясь конкретным субъектом Российской Федерации [26].

При этом особую озабоченность вызывает то, что действия нарушающих информационную безопасность лиц направлены против функционирования органов государственной власти и подведомственных им учреждений, промышленных предприятий. Новая опасная уязвимость затрагивает объекты, относящиеся к критической информационной инфраструктуре. Неуделение внимания данному вопросу несет неизгладимые последствия, поскольку затрагивает надежность функционирования, например, систем электроснабжения.

Безусловно, как в Российской Федерации, так и на уровне отдельных субъектов Российской Федерации, в том числе, например, в практике рассмотренной нами Тюменской области, органами государственной власти предпринимаются активные усилия по укреплению информационной безопасности. Это выражается не только в принятии и развитии нормативно-правовой базы в данной сфере, в частности, Федерального закона от 28.12.2010 № 390-ФЗ «О безопасности» [70], Закона Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» [16], и иных законодательных актов, но и в выработке новых эффективных механизмов и средств защиты информационной безопасности.

Новая веха развития в данной области связывается с принятием указа Президента Российской Федерации от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» [63]. В представленном

законодательном акте находят вопросы разработки и развития отечественных IT-решений в области информационной безопасности.

Таким образом, теоретическое осмысление определения и сущности информационной безопасности позволило сделать следующие выводы.

В доктрине права не сложилось единого подхода к определению данного термина. Впрочем, несмотря на плюрализм мнений в данном вопросе нельзя отрицать, что в проанализированных подходах просматриваются общие черты. В частности, это выражается в понимании информационной безопасности как неотъемлемой составляющей национальной безопасности. Определение данного термина в указанном ключе отражает современные реалии – усиление геополитической напряженности, развернутой против Российской Федерации войны в информационной пространстве.

Проведение сравнительного исследования вопроса, связанного с информационной безопасностью сквозь призму исторической эпохи, позволило провести грань между определенным историческим периодом и настоящим временем.

В результате проведенного исследования установлено, что становление и развитие информационной безопасности связывается с периодом развития древнерусского государства.

В рассматриваемый исторический период обеспечение информационной безопасности осуществлялось на основе сочетания контрольной и других форм деятельности. В частности, для защиты информации от посягательств третьих лиц применялись методы и приемы стенографии и шифрования.

В настоящее время учитывая масштаб проникновения информационно-коммуникационных технологий в жизнь современного общества, органов государственной власти и экономических субъектов, а также высокий уровень зависимости создаваемых в Российской Федерации информационных систем и ресурсов от импортозамещения, на повестку дня поставлен вопрос

обеспечения информационной безопасности страны в условиях новых вызовов и угроз.

В результате рассмотрения информационной безопасности в структуре национальной безопасности представлено определение термина «национальная безопасность», рассмотрена её содержательная структура, определено место информационной безопасности в структуре национальной безопасности. Установлено, что национальные интересы государства и общества выступают фундаментальной основой информационной безопасности. Таким образом, обеспечение информационной безопасности приобретает особую остроту, в частности, в деятельности органов государственной власти, которая тесно взаимосвязана с национальной безопасностью, учитывая участившиеся случаи компьютерных атак на информационное пространство Российской Федерации.

Последнее десятилетие в особенности обострило проблему усиления угроз в информационно-кибернетическом пространстве и использования информационных ресурсов для разрушения целостности информационной безопасности государства. При этом важно учитывать, что истоки данной проблемы связываются и с отсутствием законодательной базы в сфере защиты кибернетического пространства, возрастанием напряженности между государствами в кибернетическом пространстве.

Глава 2 Гарантии обеспечения информационной безопасности

2.1 Общие гарантии информационной безопасности

В настоящее время импортозамещение в сфере информационной безопасности государства выступает одним из приоритетных технологических направлений, ориентированных на снижение зависимости отечественных разработок от иностранных компонентов и оборудования, программного обеспечения, а также развитие в Российской Федерации отечественных IT-решений [19, с. 150]. Данное направление принимает новые очертания на фоне усиления геополитической напряженности, кибернетических угроз.

Укрепление независимости Российской Федерации в информационном пространстве позволяет нивелировать последствия, возникающие от внешних вызовов и угроз, способствует развитию киберустойчивости страны. В приведенном контексте показательно также исследование Ю.Н. Смирнова, Р.И. Фатыхова, в котором авторы приходят к выводу, что развитие высококвалифицированных кадров в области информационной безопасности выступает своего рода «фундаментом» ее обеспечения в условиях динамичного развивающихся рынков и усиления глобальных проблем и вызовов. В продолжение высказываемой мысли учеными акцентировано внимание на разработке и поддержке отечественных IT-решений, которые, по их мнению, служат основой для развития инновационных подходов к обеспечению информационной безопасности [54, с. 43].

Наглядным подтверждением высказываемому тезису служит развитие национальных криптографических технологий. К примеру, за последние несколько лет на фоне усиления геополитической напряженности и санкционного давления наблюдается активное развитие средств криптографической защиты информации [19, с. 150].

Широкое распространение они приобретают в органах государственной власти и в области обеспечения критической информационной

инфраструктуры. Активизация усилий государства и частного сектора в данном направлении способствует не только укреплению независимости страны в области информационной безопасности, но и минимизирует последствия возникающих внешних угроз.

В научно-экспертном сообществе в данном ключе высказывается мнение, что развитие отечественных решений в области информационной безопасности создает предпосылки для научно-технологического развития страны, повышает конкурентоспособность информационных технологий на мировой арене [32, с. 105].

Развитие данного направления на перспективу создает эффективный «каркас» защиты в информационном пространстве, одновременно с тем способствуя наращиванию потенциала в сфере информационных технологий.

В исследовании Р.С. Зариповой, А.А. Шакирова подчеркивается значимость инновационных, высокотехнологичных разработок научно-исследовательских центров, направленных на повышение эффективности систем защиты в информационном пространстве, развитие методов борьбы с кибернетическими угрозами [19, с. 151].

В качестве примера следует привести следующие отечественные IT-решения: «Kaspersky lab» и «Dr.Web» – программно-аппаратные решения, которые способствуют обеспечению информационной независимости, одновременно с тем повышая устойчивость IT-инфраструктуры от усиливающихся внешних вызовов и угроз. Впрочем, нельзя упускать из поля зрения то, что государство осознает значимость разработок в данной области, направляя усилия на усиление поддержки IT-бизнеса [20, с. 24]. Механизмы государственно-частного партнерства в сфере информационных технологий закладывают прочную основу для развития инновационных решений в данной области.

На страницах юридической публицистики высказывается суждение о том, что импортозамещение в области информационной безопасности отчетливо демонстрирует приверженность к снижению зависимости от

иностранных технологий, тем самым симулируя развитие инновационных подходов и решений.

В контексте усиления кибернетических угроз и участившихся случаев атак на информационное пространство Российской Федерации разработка и развитие отечественных решений в области информационной безопасности приобретает особую роль [18, с. 113].

Создание систем защиты данных в информационно-кибернетическом пространстве, развитие IT-инфраструктуры позволяет минимизировать риски нарушения и утечек конфиденциальной информации, а также способствует предотвращению возможных угроз и их негативных последствий для национальной безопасности страны.

В эпоху глобализированного мира развитые страны уделяют повышенное внимание обеспечению кибернетической безопасности, что выражается в инвестировании в разработку и развитие системы национальных аналитических центров (центров передового опыта) в области кибернетической безопасности. Это положительным образом сказывается на укреплении технического потенциала страны, разработке и развитии новых эффективных методов и инструментов в области обеспечения информационной безопасности.

В данном свете нельзя оставить без внимания принятую в Российской Федерации национальную программу «Цифровая экономика Российской Федерации». Структура национального проекта представлена шестью взаимосвязанными федеральными проектами. В их числе проект «Информационная безопасность», срок реализации которого – 2018-2024 гг., в рамках которого предусмотрен комплекс системных мер, направленных на его реализацию:

Прежде всего, показательны действия органов государственной власти Российской Федерации на мировой арене, выраженные во внесении проектов соглашений и конвенций, направленных на обеспечение информационного равенства в современном глобальном информационном пространстве.

Сплочение и консолидация усилий международного сообщества против глобальных угроз информационной безопасности как вызова современной стратегической стабильности в условиях современного миропорядка послужило ориентиром принятых по инициативе Российской Федерации резолюций Генеральной Ассамблеи Организации Объединенных Наций «Достижения в сфере информатизации» от 05.12.2018 [52].

Принимая во внимание тот факт, что от устойчивости функционирования информационных сетей зависит качество государственного и муниципального управления и взаимодействия органов государственной власти, в рамках правового поля федеральным законодателем закреплены определенные требования к обеспечению целостности, устойчивости функционирования и общей безопасности связи и сетевого оборудования, как для государственных информационных сетей (сокращенно – ГИС), так и для экономических субъектов, вне зависимости от их организационно-правовой формы.

Учитывая усиливающиеся риски удаленных сетевых атак в рамках национального проекта разработаны и активно внедряются меры, направленные на мониторинг сетевой IT-инфраструктуры. Кроме того, в рамках принятого национального проекта изменения затрагивают процесс проектирования, управления и эксплуатации сетей связи общего пользования с учетом современной модели внешних вызовов и угроз.

Принимая во внимание направленность и характер задач, поставленных в рамках национального проекта в целом и формирование информационной повестки дня, органами государственной власти реализована концепция «Умный город».

Среди внедренных и доказавших эффективность проектов, направленных на обеспечение защиты отдельной личности, общества и государства, в особенности следует отметить государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак

(сокращенно – ГосСОПКА), регулирование и координация деятельности которой возложена на ФСБ РФ [13, с. 144; 14, с. 101].

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, разработанная во исполнение указа Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [62], предназначена для решения следующих задач в области информационной безопасности:

- прогнозирование внешних рисков и угроз, характера и интенсивности атак на информационные системы;
- взаимодействие органов государственной власти и представителей бизнес-сообщества для выявления, предупреждения и нивелирования последствий атак в информационной среде;
- мониторинг уровня защищенности безопасности в информационной среде;
- анализ и расследование инцидентов в области информационного пространства.

Стоит заметить, что для борьбы с кибернетическими атаками и предотвращения их негативных последствий центры управления и мониторинга оснащены специальными программно-аппаратными средствами и инструментами.

В научном исследовании Л.А. Кравченко и Д.В. Субоч приводится суждение о том, что на перспективу государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак станет координатором отражений внешних атак на информационную систему.

Кроме того, в представленном исследовании акцентировано внимание на введении Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации в эксплуатацию в связи с

геополитической напряженностью информационной системы мониторинга фишинговых сайтов. В качестве положительных аспектов функционирования данной системы отмечается своевременное выявление интернет-ресурсов, на которых приведена недостоверная информация. Сведения об обнаруженных нарушениях направляются в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникация для принятия превентивных мер.

С развитием законодательства в области информационной безопасности информационная система мониторинга, как приводится в исследовании Л.А. Кравченко, Д.В. Субоч, станет полноценной платформой межведомственного взаимодействия в целях оперативного выявления и реагирования на внешнее угрозы [31, с. 40].

В рамках рассмотрения вопроса, связанного с общими гарантиями информационной безопасности, нельзя оставить без внимания переход органов государственной власти на использование отечественных онлайн-сервисов. Например аналогом мобильного приложения для обмена сообщения «WhatsApp» в настоящее время является кросплатформенный мессенджер «MAX».

На фоне санкционного давления программы и решения «Microsoft Office» заменены отечественный сервисом «Документы».

Кроме того, в связи с блокировкой в Российской Федерации некоторых зарубежных онлайн-сервисов деятельность отечественных разработчиков приобрела новый импульс и новые масштабы. Например, аналогом электронной платежной системы «PayPal» выступает платежная система «Miraclepay», создателем которой является «Яндекс».

В вопросе стимулирования импортозамещения государство предпринимает активные действия, направленные на поддержку отечественных разработок в сфере обеспечения информационной безопасности, что способствует их развитию и повышению конкурентоспособности. Впрочем, несмотря на это, нельзя исключать

некоторые проблемные «зоны». В исследовании И.А. Бирюкова в качестве проблем приводится указание на существенные затраты, связанные с разработкой и введением в эксплуатацию отечественных IT-решений. Кроме того, автор акцентирует внимание на недостаточный функционал отечественных решений и их «незрелость» [4, с. 74].

Однако не стоит упускать из поля зрения то обстоятельство, что импортозамещение представляет собой сложный и довольно затратный процесс, который требует консолидации усилий органов государственной власти, представителей частного сектора и иных субъектов. Впрочем, нельзя отрицать положительные результаты в данном направлении. Так, в 2022-2024 гг. заметна тенденция увеличения количества бюджетных мест в высших учебных заведениях по направлениям подготовки специалистов в сфере IT [4, с. 74].

Таким образом, рассмотрение общих гарантий информационной безопасности, основывающееся на изучении роли импортозамещения в условиях новых вызовов и усиливающихся угроз в информационном пространстве, а также в контексте принятого и реализуемого в Российской Федерации национального проекта «Цифровая экономика», позволило прийти к следующим выводам.

Импортозамещение в сфере информационной безопасности выступает одним из приоритетных технологических направлений, ориентированным на снижение зависимости от иностранных компонентов и оборудования, программного обеспечения, а также развитие отечественных IT-решений. Данное направление принимает новые очертания на фоне усиления геополитической напряженности, кибернетических угроз.

В эпоху глобализированного мира развитые страны уделяют повышенное внимание обеспечению безопасности в информационно-кибернетическом пространстве, что выражается в инвестировании в создание и развитие системы национальных центров передового опыта области кибербезопасности. В Российской Федерации принята и реализуется

национальная программа «Цифровая экономика Российской Федерации», структуру которой образует шесть национальных проектов, в том числе «Информационная безопасность». В целом показатели, предусмотренные в рамках реализации национального проекта, ориентированы на минимизацию рисков утечек конфиденциальной информации, предотвращение возможных угроз и их последствий для национальной безопасности Российской Федерации.

2.2 Организационные гарантии информационной безопасности

Раскрытие содержания данного параграфа следует предварить высказыванием о том, что активное взаимодействие органов государственной власти и управления на региональном и федеральном уровнях по вопросам исполнения законодательства Российской Федерации, актов Президента Российской Федерации и Правительства Российской Федерации в области обеспечения информационной безопасности становится одним из перспективных направлений в контексте обеспечения стратегических приоритетов страны.

Анализируя вопросы, связанные с организационными гарантиями информационной безопасности, стоит заметить их многогранный характер, который отчетливо просматривается во внутриполитических и внешнеполитических векторах.

Во внутриполитической сфере деятельность органов государственной власти сосредоточена на предотвращении несанкционированного доступа и внешних вызовов, связанных с воздействием на функционирование информационной системы, а также обеспечение информационной безопасности в контексте каналов связи для выстраивания электронного взаимодействия территориальных органов государственной власти.

Нельзя не отметить и консолидацию усилий органов государственной власти в направлении предотвращения снижения показателей эффективности

деятельности государственных и муниципальных учреждений, выраженных в разработке и реализации комплекса мер, направленных на противодействие утечки информации, несанкционированного воздействия на IT-инфраструктуру.

Отдельного внимания заслуживает и обеспечение информационной безопасности органами государственной власти в отдельных научно-технических областях. В приведенном контексте стоит отметить наращивание усилий в направлении предотвращения утечки информации, связанной с фундаментальными, поисковыми и прикладными научно-техническими исследованиями, новыми технологиями и решениями, которые служат стратегическим ресурсом развития как отдельно взятого субъекта Российской Федерации, так и страны в целом.

Представляется, что деятельность органов государственной власти в рамках обеспечения информационной безопасности в рамках внутриполитического курса связывается с функционалом деятельности отдельных органов. В данном ключе показательна позиция ученых, которые предлагают руководствоваться пятиступенчатой «моделью» деятельности органов государственного управления в данном направлении:

Во-первых, организационно-правовое и методическое обеспечение защиты информации и IT-систем, в том числе, сведений, которые носят ограниченный доступ.

Во-вторых, обеспечение физической безопасности информационных ресурсов (многообразие технических средств, каналов связи) от возможного внешнего воздействия в результате циркуляции информационных потоков.

В-третьих, обеспечение защиты информации от внешнего несанкционированного доступа, а также её движения с соблюдением принципа обеспечения конфиденциальности и недопустимости нарушения её целостности.

В-четвертых, обеспечение безопасности информационных ресурсов (защита от вредоносного программного обеспечения).

В-пятых, совершенствование информационной безопасности органов государственного управления [38, с. 164].

В настоящее время органы государственной власти уделяют повышенное внимание разработке и реализации мер и мероприятий, ориентированных на реализацию признанных Конституцией Российской Федерации прав личности в условиях развивающегося информационного общества, в том числе возможности в осуществлении свободного поиска, передачи, производства информации.

В приведенном контексте нельзя оставить без внимания и реализацию иных субъективных прав в информационной среде, которые предусмотрены статьей 23 Конституции Российской Федерации [29].

При этом органы государственного управления сосредотачивают особое внимание на недопустимости циркуляции информации, которая носит ограниченный доступ. Повышенное внимание к данной проблеме обнаруживается и в рамках законодательной плоскости. В частности, здесь следует уделить внимание опыту законодателя Тюменской области, которым утверждено Положение об информационной безопасности исполнительных органов государственной власти Тюменской области, подведомственных ему учреждений [50], государственной программы Тюменской области «Развитие информатизации», в рамках которой предусмотрен ряд последовательных задач:

- создание устойчивой и безопасной IT-инфраструктуры высокоскоростной передачи, обработки и хранения данных преимущественно на основе отечественных решений в области информационных технологий, разработка и внедрение инструментальных цифровых решений в деятельность органов государственного управления;
- создание информационной инфраструктуры для обеспечения широкополосным доступом к сети Интернет социально значимых объектов, функционирующих на территории Тюменской области.

В условиях усиливающихся внешних вызовов и угроз органы государственного управления придерживаются концепта информационной открытости. Однако признавать полностью совершенной деятельность органов государственной власти в данном направлении нельзя. Крайне острым и чувствительным вопросом выступает импортозамещение и последствия, вызванные переходом рынка на отечественные решения и средства защиты информации. Однако более глубинному пониманию данной проблемы и иных взаимосвязанных с ней проблемных аспектов будет посвящена третья глава выпускной квалификационной работы.

Помимо организационного обеспечения информационной безопасности в деятельности органов государственной власти также важно не упускать из поля зрения и программно-техническое обеспечение. И это весьма небезосновательно в контексте усиливающегося внешнего воздействия в информационном пространстве.

Одним из требований к программно-техническому обеспечению, в том числе, образующих его содержание средств защиты информации, выступает сертификация, организуемая уполномоченными органами – Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю. Обязательной сертификации подлежат программно-аппаратные средства, средства криптографической защиты информации (сокращенно – СКЗИ), средства обнаружения вредоносных программ, а также средства защиты информации от внешнего несанкционированного воздействия.

При отсутствии в рамках информационной системы сведений, отнесенных в порядке, предусмотренном законодательством, к сведениям ограниченного доступа (то есть сведениям, составляющим государственную тайну), то внедрение и эксплуатация совокупности средств IT-защиты осуществляется согласно положениям, изложенным в Приказе Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей

государственную тайну, содержащейся в государственных информационных системах» [49].

Рассматривая организационные гарантии информационной безопасности вновь следует уделить внимание опыту Тюменской области. И здесь следует отметить переход органов государственного и муниципального управления на централизованную информационную архитектуру, который связывается с 2014 годом [36]. На фоне «взятия курса» на IT-инфраструктуру деятельность органов публичной власти в области информационной безопасности приобретает новые очертания: развитие механизмов межведомственного взаимодействия в электронной форме; развитие единого информационного ресурса в зависимости от поставленных задач в области электронного документооборота государственного и муниципального управления (электронного правительства), подключение к системе всех звеньев государственного и муниципального управления, автоматизация деятельности.

В дополнительном освещении в рамках данного параграфа также нуждается вопрос, связанный с обеспечением информационной безопасности в деятельности органов государственного и муниципального управления в Тюменской области, в условиях новых вызовов и угроз.

В частности, по данным, представленным на конец 2024 года перевод органов государственного и муниципального управления Тюменской области на отечественное программное обеспечение выполнен на 80% [9].

При этом представленные официальные данные позволяют сделать вывод о расширении перечня государственных информационных систем. Их количество по итогам 2024 года составило 19 информационных систем.

В качестве положительного аспекта стоит отметить осуществление полного перевода социально значимых услуг. Как следует из апробированных данных, основная часть среди них представлена следующим образом: запись детей на дополнительные занятия; вопросы, связанные с назначением и

выплатой средств из материнского (семейного) капитала; вопросы назначения и получения выплат не несовершеннолетних детей.

Кроме того, в условиях новой геополитической реальности особенно актуальным выступает вопрос, связанный с повышением квалификации сотрудников государственных и муниципальных учреждений, ответственных за защиту информационной безопасности. В данном ключе стоит отметить, что на территории Тюменской области за 2021-2024 гг. обучение пройдено более 450 сотрудниками.

На территории Тюменской области как в одном из передовых регионов в контексте показателя цифровой зрелости активно осуществляется реализация широкого ряда государственных программ, национальных и федеральных проектов в ключевых отраслях экономики и социальной сфере.

Особое внимание в эпоху цифровых трансформаций уделяется государственному и муниципальному управлению в части IT-инфраструктуры, повышения процессов разработки и принятия государственных решений, обеспечения информационной безопасности от внешнего воздействия.

Так, информационная система «Единый центр хранения и обработки данных систем видеонаблюдения Тюменской области» (сокращенно – ЕЦХД СВН ТО) по состоянию на 01.01.2024 г. представлена более 4 тыс. камерами, из которых 1/4 часть территориально расположена в муниципальных образования Тюменской области [25].

Используемое организационно-информационное обеспечение государственного и муниципального управления в Тюменской области носит широкую направленность, включая: концепцию электронного правительства, автоматизированную информационную систему Тюменской области «Единая мобильная платформа Тюменской области», Единую систему межведомственного электронного взаимодействия, официальный портал органов государственной власти Тюменской области, инструментальные цифровые платформы и др.

Растущие внешние угрозы и усиление геополитической напряженности заставили пересмотреть подходы к обеспечению информационной безопасности. В данном ключе стоит отметить повышение спроса на аппаратное и программное обеспечение с расширенными аналитическими функциями. Безусловно, изменения к организации обеспечения информационной безопасности требуют новых, инновационных подходов в решении данного вопроса.

В условиях интенсивного развития информационно-коммуникационных технологий органы государственной власти и представители частного сектора уделяют повышение внимание вопросам автоматизации, интеграции нейроенных сетей и алгоритмов, разработанных на базе машинного обучения в процессы обеспечения информационных систем и компьютерных сервисов.

Особое внимания в связи с усилением санкционного давления уделяется безопасности логистической цепи поставок, внедрению решений и инструментов отечественных разработок во все сферы деятельности. На фоне возрастания внешних угроз безопасности персональных данных особую актуальность приобретает технология искусственного интеллекта.

Как приводится в исследовании О.А. Озакман, подход органов государственной власти и представителей бизнес-структур смещается в направлении использования технологии искусственного интеллекта с целью обнаружения и предотвращения атак в рамках информационно-кибернетического пространства [35, с. 230]. При этом в данном вопросе заслуживает внимания и аналитическое исследование «Mordor Intelligence», в котором приводится, что объем мирового рынка систем и технологий искусственного интеллекта в сфере информационной безопасности продемонстрирует рост с 21,2 млрд. долл. США в 2023 году до 50,6 млрд. долл. США к 2028 году [77].

Объем вложений в обеспечение безопасности в информационно-кибернетическом пространстве и защита персональных данных в 2024 году составил 5,5 млн. долл. США [77].

Технологии искусственного интеллекта и расширенные аналитические функции существенно повышают эффективность решений в области обеспечения информационной безопасности. Инновационные подходы находят применение в наиболее востребованных технических решениях, в том числе, в сфере защиты от вредоносных программ, защиты от утечек персональных данных, системах обнаружения инцидентов информационной безопасности, аномальных активностей в сетях передачи данных, системах фрод-мониторинга и др.

В качестве положительных аспектов их использования стоит отметить контроль доступа пользователей к информационным ресурсам, выявление фактов несанкционированного доступа и несанкционированных действий, мониторинг уязвимостей и оценка их применимости, разработку эффективных антивирусных решений.

Именно при обработке огромного массива данных результаты исследования нейронных сетей не сопоставимы с другими технологическими решениями.

Посредством автоматизации реагирования на инциденты информационной безопасности происходит сокращение времени на принятие решений на внешние атаки. Также в данном контексте стоит отметить снижение рисков человеческого фактора.

Технология искусственного интеллекта позволяет обнаружить аномальные активности, которые указывают на кибернетические угрозы [24]. Обработка массива данных позволяет выявить тренды и внешние угрозы, сфокусировав внимание на блокировании зашифрованного трафика для скрытия вредоносной активности, автоматизации мониторинга уязвимостей в информационных системах [65]. Кроме того, инновационные инструменты направлены на осуществление мониторинга показателей поведенческих реакций пользователей при взаимодействии с информационными системами [23].

Таким образом, обеспечение информационной безопасности в деятельности органов государственной власти неразрывно связано с вопросами организационного обеспечения (организационных гарантий).

Во внутриполитической сфере деятельность органов государственной власти сосредоточена на предотвращении несанкционированного доступа и внешних вызовов, связанных с воздействием на функционирование информационной системы, а также обеспечение информационной безопасности в контексте каналов связи для выстраивания электронного взаимодействия территориальных органов государственной власти.

Деятельность органов государственной власти в рамках внешнеполитического курса носит многогранный характер, поскольку не очерчивается исключительно повышением эффективности и сбалансированности развития IT-инфраструктуры, но и развивается в области обеспечения рационального использования информационных ресурсов.

2.3 Нормативные гарантии информационной безопасности

Раскрытие содержания данного параграфа следует предварить указанием на то, что основополагающим актом в области обеспечения информационной безопасности является Стратегия развития информационного общества, утвержденная указом Президента Российской Федерации от 09.05.2017 № 203 и рассчитанная на период 2017-2030 гг. [61]. В ней определены цели и коррелирующие ей задачи и меры по реализации внутренней и внешней политики государства в сфере применения информационно-коммуникационных технологий, направленных на информатизацию гражданского общества, обеспечение национальных интересов и реализацию приоритетов признанных стратегически приоритетными.

Основными принципами Стратегии являются:

– обеспечение прав граждан на доступ к информации;

– обеспечение свободы выбора средств получения знаний при работе с информацией;
– сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг;
– приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий;
– обеспечение законности и разумной достаточности при сборе, накоплении и распространении информации о гражданах и организациях;
– обеспечение государственной защиты интересов российских граждан в информационной сфере.

Другим ключевым нормативно-правовым актом в области обеспечения информационной безопасности является Доктрина информационной безопасности.

Стоит заметить, что определенно новую веху развития в области обеспечения информационной безопасности ознаменовало утверждение Национальной программы «Цифровая экономика Российской Федерации» [39].

Целями представленной программы являются:

– создание экосистемы цифровой экономики Российской Федерации, в которой данные в цифровой форме являются ключевым фактором производства во всех сферах социально-экономической деятельности и в которой обеспечено эффективное взаимодействие, включая трансграничное, бизнеса, научно-образовательного сообщества, государства и граждан;
– создание необходимых и достаточных условий институционального и инфраструктурного характера, устранение имеющихся

препятствий и ограничений для создания и (или) развития высокотехнологических бизнесов и недопущение появления новых препятствий и ограничений как в традиционных отраслях экономики, так и в новых отраслях и высокотехнологичных рынках;

– повышение конкурентоспособности на глобальном рынке как отдельных отраслей экономики Российской Федерации, так и экономики в целом.

Цифровая экономика представлена тремя следующими уровнями, которые в своем тесном взаимодействии влияют на жизнь граждан и общества в целом:

– рынки и отрасли экономики (сферы деятельности), где осуществляется взаимодействие конкретных субъектов (поставщиков и потребителей товаров, работ и услуг);
– платформы и технологии, где формируются компетенции для развития рынков и отраслей экономики (сфер деятельности);
– среда, которая создает условия для развития платформ, технологий и эффективного взаимодействия субъектов рынков и отраслей экономики (сфер деятельности) и охватывает нормативное регулирование, информационную инфраструктуру, кадры и информационную безопасность.

Реализация данной программы требует тесного взаимодействия государства, бизнеса и науки, так как основным результатом ее реализации должно стать создание не менее 10 национальных компаний-лидеров – высокотехнологичных предприятий, развивающих «сквозные» технологии и управляющих цифровыми платформами, которые работают на глобальном рынке и формируют вокруг себя систему «стартапов», исследовательских коллективов и отраслевых предприятий, обеспечивающую развитие цифровой экономики.

Структура национального проекта содержательно представлена шестью федеральными проектами. В их числе проект «Информационная безопасность».

Проект «Информационная безопасность» ориентирован на обеспечение информационной безопасности на основе внедрения и реализации отечественных IT-решений, гарантирующих защиту общественных и частных интересов.

На период реализации национального проекта «Информационная безопасность» предусмотрено:

- предоставление поддержки экспортно-ориентированным субъектам малого и среднего предпринимательства (МСП), что позволит обеспечить устойчивое присутствие национальных IT-решений и подходов на международной арене;
- достижение маршрутизации трафика в сети Интернет на территории Российской Федерации;
- обеспечение населения Российской Федерации средствами защиты информации.

Среди показателей эффективности национального проекта «Информационная безопасность» в цифровом выражении:

- снижение усредненного показателя простоя государственных информационных систем (сокращенно – ГИС) в результате атак на информационные ресурсы с 65 часов на 31.12.2018 г. до 1 часа на 31.12.2024 г.;
- повышение доли населения Российской Федерации, которое используют для защиты информации специальные программно-аппаратные средства защиты и инструменты отечественного производства с 86% на 31.12.2018 г. до 97% на 31.12.2024 г.;
- увеличение количества подготовленных специалистов по образовательным программам в области ИБ с 7 000 до 24 000 тыс.;

– снижение доли иностранного программного обеспечения в общем объеме закупок, осуществляемых органами государственной власти, в процентном выражении – от 50% до 10%.

Таким образом, в настоящее время в Российской Федерации в условиях новой геополитической реальности эффективно реализуется государственная политика в сфере обеспечения информационной безопасности. В качестве положительного аспекта следует отметить усовершенствованный подход к механизму взаимодействия органов государственной власти и общества в данной области.

В качестве подтверждения правоты данного тезиса следует отметить общественное обсуждение Закона о «суверенном Рунете» [51, с. 94].

Вынесение представленного законопроекта на общественное обсуждение позволило не только внести коррективы в ряд направлений, проводимой органами государственной власти политики, но и повысить информированность граждан о совершаемых органами государственного и муниципального управления действиях, что подчеркивает публичную открытость государства.

Таким образом, подводя итог ко второй главе выпускной квалификационной работы, следует сформулировать следующие выводы.

Рассмотрение общих гарантий информационной безопасности, основывающееся на изучении роли импортозамещения в условиях новых вызовов и угроз, а также в контексте принятого и реализуемого в Российской Федерации национального проекта «Цифровая экономика», позволило прийти к следующим выводам.

Импортозамещение в сфере информационной безопасности выступает одним из приоритетных технологических направлений, ориентированным на снижение зависимости от иностранных компонентов и оборудования, программного обеспечения, а также развитие отечественных IT-решений. Данное направление принимает новые очертания на фоне усиления геополитической напряженности, кибернетических угроз.

В эпоху глобализированного мира развитые страны уделяют повышенное внимание вопросу обеспечения безопасности в информационно-кибернетическом пространстве, что выражается в инвестировании в создание и развитие системы национальных центров передового опыта области кибербезопасности. В Российской Федерации принята и реализуется национальная программа «Цифровая экономика Российской Федерации», структуру которой образует шесть национальных проектов, в том числе «Информационная безопасность».

В целом показатели, предусмотренные в рамках реализации национального проекта ориентированы на минимизацию рисков утечек конфиденциальной информации, предотвращение возможных угроз и их последствий для национальной безопасности Российской Федерации.

В результате рассмотрения организационных гарантий информационной безопасности установлено, что во внутриполитической сфере деятельность органов государственной власти сосредоточена на предотвращении несанкционированного доступа и внешних вызовов, связанных с воздействием на функционирование информационной системы, а также обеспечение информационной безопасности в контексте каналов связи для выстраивания электронного взаимодействия территориальных органов государственной власти.

Деятельность органов государственной власти в рамках внешнеполитического курса носит многогранный характер, поскольку не очерчивается исключительно повышением эффективности и сбалансированности развития IT-инфраструктуры, но и развивается в области обеспечения рационального использования информационных ресурсов.

Кроме того, растущие внешние угрозы и усиление геополитической напряженности заставили пересмотреть подходы к обеспечению информационной безопасности. В данном ключе стоит отметить повышение спроса на аппаратное и программное обеспечение с расширенными аналитическими функциями. Безусловно, изменения к организации

обеспечения информационной безопасности требуют новых, инновационных подходов в решении данного вопроса.

В условиях интенсивного развития информационно-коммуникационных технологий органы государственной власти и представители частного сектора уделяют повышение внимание вопросам автоматизации, интеграции нейроенных сетей и алгоритмов, разработанных на базе машинного обучения в процессы обеспечения информационных систем и компьютерных сервисов.

Изучение вопроса, связанного с нормативными гарантиями информационной безопасности, позволило отметить Стратегию развития информационного общества, утвержденную указом Президента Российской Федерации от 09.05.2017 № 203 и рассчитанную на период 2017-2030 гг. В ней определены цели и коррелирующие ей задачи и меры по реализации внутренней и внешней политики государства в сфере применения информационно-коммуникационных технологий, направленных на информатизацию гражданского общества, обеспечение национальных интересов и реализацию приоритетов признанных стратегически приоритетными.

Другим ключевым нормативно-правовым актом в области обеспечения информационной безопасности является Доктрина информационной безопасности.

Глава 3 Проблемы и перспективы обеспечения информационной безопасности

3.1 Проблемы обеспечения информационной безопасности

В условиях усиления новых вызовов и внешних угроз проблема обеспечения информационной безопасности приобретает особую актуальность.

В Российской Федерации вопросы, связанные с обеспечением безопасности в информационном пространстве, как следует из результатов проведенного исследования, затрагивают деятельность органов государственной власти и подведомственных им учреждений.

Однако принятая в Российской Федерации многоуровневая иерархия органов государственной власти, деятельность которых направлена на обеспечения информационной безопасности, подвергается критике среди представителей научно-экспертного сообщества, которые обосновывают целесообразность создания Единого центра управления информационной безопасностью [456, с. 1203].

Впрочем, не вдаваясь в полемику относительно высказываемого суждения, следует отметить, что вопрос обеспечения информационной безопасности носит крайне чувствительный характер и достаточно остро стоит на повестке дня, учитывая новые вызовы и угрозы в данной области. Особую тревогу вызывают следующие вопросы.

Во-первых, кадровый дефицит на IT-рынке.

По данным Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, представленным в 2024 году, дефицит квалифицированных кадров в IT-отрасли оценивается в 700 тыс. [53].

Данная проблема находится в центре особого внимания органов государственной власти, что подтверждает реализация проекта подготовки

специалистов в сфере IT-технологий на основе разработки новых образовательных программ [42].

Кроме того, нельзя оставить без внимания и анонсированный в 2020 году проект «Цифровые профессии», который предоставляет гражданам возможность в получении дополнительного образования в сфере информационных технологий. На перспективу до 2030 году данный показатель составит порядка 1,2 млн. человек [6].

Другим актуальным вопросом является несовершенство системы защиты персональных данных. Несмотря на повышенное внимание органов государственной власти к данной проблеме, вопрос утечки информации остается крайне острым.

Негативные последствия носят неизгладимый характер, поскольку затрагивают не только субъективные права, но и подрывают доверие населения к деятельности органов государственной власти.

Кроме того, стоит отметить и тенденцию, свидетельствующую об интенсивном росте масштаба утечек персональных данных. Согласно данным, представленным отечественным разработчиком IT-решений «InfoWatch» в 2024 году в Российской Федерации зафиксировано более 1,5 млрд. случаев утечки персональных данных, что превышает показатель 2023 года на 31,7% [76].

Крайне чувствительным вопросом является также несовершенство информатизации социальной работы. Обеспечение информационной безопасности в социальной сфере – одно из приоритетных направлений в деятельности органов государственной власти. Однако реализация деятельности по данному направлению сопряжена с рядом проблем, вызванных широким проникновением иностранных программ и приложений, преобладающими среди населения Российской Федерации, низким уровнем осведомленности граждан в области информационной безопасности.

Появляются новые угрозы и вызовы обеспечения информационной безопасности в условиях усиливающейся геополитической напряженности. В

последнее десятилетие проблемы и процессы в кибернетическом пространстве приобретают новые очертания, подрывая основы информационной безопасности страны.

Данные проблемы связывается с отсутствием внимания к регулированию сферы кибернетического пространства, усилением напряженности между государствами в кибернетическом пространстве.

Особую тревогу вызывает и ослабление взаимодействие в вопросах обеспечения защиты в кибернетическом пространстве на международном уровне, и как следствие – неэффективность механизмов, платформ и площадок для ведения многостороннего диалога.

Актуализированные на 2024 год статистические данные свидетельствует о росте кибернетических атак на 39% в сравнении с 2023 годом [8]. Однако особую остроту вызывает то обстоятельство, что действия лиц направлены против функционирования органов государственного и муниципального управления, подведомственных им учреждений, промышленных предприятий.

Новые угрозы в информационно-кибернетическом пространстве затрагивают деятельность объектов, которые отнесены к объектам критической IT-инфраструктуры. Отсутствие должного внимания к регулированию данного вопроса несет серьезные последствия. Это обуславливается их воздействием на устойчивость и надежность функционирования объектов критической IT-инфрастурктуры.

Однако проблемы в области обеспечения информационной безопасности актуальны не только для Российской Федерации, но и для всего мирового сообщества.

Согласно данным, представленным Центром стратегических и международных исследований, ущерб от преступлений в сфере информационных технологий, оценивается в 450 млрд. долл. [21].

Угрозы информационной безопасности на международном уровне связываются с:

- программными и аппаратными сбоями в программно-аппаратного обеспечении;
- техническими неисправностями программно-аппаратного обеспечения, вызванного нарушениями и сбоями в электрических сетях, в том числе, информационными провокациями, а также конструктивными неисправностями;
- модификацией вирусов и вредоносных программ;
- непреднамеренным халатным отношением сотрудников в области обеспечения информационной безопасности.

Нельзя оставить без внимания и инструменты, используемые для нарушения целостности информационных систем.

Так, например, известно вредоносное программное обеспечение «Ransomware». При запуске программного обеспечения нарушается работоспособность технического объекта. Для восстановления работоспособного состояния объекта разработчики вредоносной программы направляют требование об оплате, как правило, в форме цифровой валюты для невозможности отслеживания транзакций.

Опасны и программы, имитирующее удаление вредоносного программного обеспечения.

Выделяется агрессивный рекламный софт «Madware», направленный на повреждение программного обеспечения мобильных устройств.

Наблюдается в настоящее время и Кибербуллинг или использование информационных атак для воздействия на пользователей в виртуальном пространстве.

В зоне повышенного риска находятся персональные компьютеры и мобильные устройства граждан, которые не уделяют должного внимания вопросам обеспечения информационной безопасности. Особую тревогу вызывает тенденция роста рынка киберпреступных сервисов.

Так, согласно данным, представленным «Search Inform», в странах Западной Европы на протяжении последних лет цена предложения на

проведение DDoS-атаки увеличилась с 3 до 12 млн. долл. При этом при совершении кибернетической атаки на объекты критической инфраструктуры цена повышается в несколько раз [21].

В Российской Федерации динамика преступлений в информационно-кибернетическом пространстве не столь выраженная. Однако несмотря на это, нельзя исключать другие проблемы в области обеспечения информационной безопасности.

Как приводится в исследовании отечественного разработчика IT-решений «Инфарс» одним из уроков, извлеченных из кризисных ситуаций, вызванных усилением геополитической разбалансированности мира, послужило понимание значимости своевременного и регулярного обновления программно-аппаратного обеспечения. Это связывается с ростом кибернетических атак вследствие уязвимости операционных систем. Например, кибернетические атаки на операционную систему «Windows Server», для которой присущ уязвимость высокой степени риска [37].

Другая актуальная проблема связывается с распространением удаленной занятости. Как приводится в исследовании «Инфарс» с переводом сотрудников на дистанционную занятость наблюдается усиление интереса к использованию VPN-сервисов и других инструментов для обеспечения доступа к корпоративным сетям. Однако данные инструменты подвержены критической уязвимости, вследствие чего повышаются риски утечки персональных данных [37].

Органы государственной власти осознают последствия усиления новых вызовов и угроз в информационно-кибернетическом пространстве, формируя новые механизмы регулирования в области обеспечения информационной безопасности. Показательным является опыт законодателя Китайской Народной Республики, в частности, принятие Закона о кибербезопасности, регулирующего создание, эксплуатацию, обслуживание и использование сетей, а также надзор и администрирование процедур кибербезопасности на территории страны [30].

Нельзя оставить без внимания и проблемы, связанные с несовершенством законодательства Российской Федерации, в условиях новых вызовов и усиления угроз в информационно-кибернетическом пространстве.

Таким образом, проведенное исследование позволило выявить ряд актуальных проблем в области обеспечения информационной безопасности. В частности, особое внимание обращено на следующие проблемы:

- кадровый дефицит на IT-рынке;
- другим актуальным вопросом является несовершенство системы защиты персональных данных. Несмотря на повышенное внимание органов государственной власти к данной проблеме, вопрос утечки информации остается крайне острым;
- крайне чувствительным вопросом является несовершенство информатизации социальной работы. Обеспечение информационной безопасности в социальной сфере – одно из приоритетных направлений в деятельности органов государственной власти. Однако реализация деятельности по данному направлению сопряжена с рядом проблем, вызванных широким проникновением иностранных программ и приложений, преобладающими среди населения Российской Федерации, низким уровнем осведомленности граждан в области информационной безопасности;
- новые угрозы и вызовы обеспечения информационной безопасности в условиях усиливающейся геополитической напряженности;
- несовершенство законодательства Российской Федерации в условиях новых вызовов и усиления угроз в информационно-кибернетическом пространстве.

В целом, представленные в рамках данного исследования проблемы обеспечения информационной безопасности в условиях новых вызовов и угроз приобретает другие очертания, обуславливая необходимость комплексного подхода к их решению.

3.2 Перспективы и предложения в области обеспечения информационной безопасности

В условиях новых вызовов и угроз, усиления геополитической разбалансированности мира с учетом выявленных в рамках проведенного исследования проблем важно активизировать усилия в направлении совершенствования обеспечения информационной безопасности страны, в том числе уделить внимание следующим вопросам:

– защите объектов критической IT-инфраструктуры;

– совершенствованию механизмов обнаружения и предотвращения внешнего вредоносного воздействия на информационно-кибернетическое пространство;

– а также подготовке квалифицированных кадров в области цифровых технологий, информации и информационной безопасности.

Кроме того, целесообразна разработка новых методов и средств защиты информационной безопасности. Однако предлагаемая мера сопряжена с угрозами сбора, накопления, хранения и обработки информации в информационных системах. В частности, данная проблема усиливается на фоне появления и интенсивного развития новых средств и методов защиты, которая сопряжена с оценкой их качества и эффективности. Также в рамках данного направления необходимо сконцентрировать внимание на разработке критериев, на основе которых будет производится оценка их качества и эффективности.

В качестве другого направления в вопросе совершенствования обеспечения информационной безопасности следует выделить разработку и внедрение в деятельность органов государственного и муниципального управления новых информационных технологий. Однако при их внедрении особое внимание следует уделить вопросу их защищенности.

Целесообразность данного предложения обуславливается тем, что совершенствование государственного и муниципального управления в

условиях новых вызовов и угроз сопряжено с необходимостью разработки новых концептуальных принципов построения функциональных узлов цифровой системы и организации взаимодействия данных узлов. Данная проблема особенна актуальна для определенных субъектов Российской Федерации, в том числе, Тюменской области. Это объясняется циркуляцией широкого объема информационных потоков. Одновременно с тем следует указать и на другую проблему, связанную с тем, что уровень научно-поисковых исследований в регионе в данном вопросе крайне низок. В данной связи обоснованность данного предложения не вызывает сомнения.

Другим направлением совершенствования обеспечения информационной безопасности послужит создание на региональном уровне целостной и многоуровневой системы защищенного электронного документооборота с уклоном на электронную цифровую подпись. Однако при внедрении данного предложения стоит уделить внимание контролю целостности информации.

В области правовой политики в сфере информационной безопасности следует уделить внимание вопросам повышения безопасности, хранения и обработки данных российских операторов персональных данных, которые в условиях геополитической напряженности приобретают крайнюю чувствительность. В данной связи в рамках правового поля целесообразно закрепить положение, связанное с установлением обязательной сертификации услуг в области облачного хранения и обработки персональных данных. Автор выпускной квалификационной работы обосновывает необходимость внесения изменений в Федеральный закон «О персональных данных» путем закрепления статьи 18.2 «Сертификация облачных сервисов». В рамках данной статьи предлагается закрепить следующее положение: «При сборе персональных данных оператор обязан использовать аккредитованные государством в соответствии с законодательством Российской Федерации облачные сервисы и технологии. Выдача сертификата осуществляется органами исполнительной власти по согласованию с Федеральной службой

Российской Федерации и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации».

Кроме того, для усиления информационной безопасности в динамично развивающемся информационно-кибернетическом пространстве следует поставить на повестку дня вопрос о внесении изменения в Федеральный закон «О персональных данных», направленного на своевременное выявление и устранение уязвимых мест в системе обработки персональных данных. В контексте предлагаемой новеллы автор выпускной квалификационной работы признает целесообразным расширить обязанности контролирующих органов путем закрепления в рамках правового поля проведения обязательного аудита внутренних процессов обработки данных. В данной связи обосновывается необходимость дополнения представленного Федерального закона ст. 19.1 «Аудит информационной безопасности», в рамках которой следует закрепить положение: «Операторы персональных данных обязаны ежегодно проводить независимый аудит системы обработки данных с привлечением к данному процессу аккредитованных профессиональных аудиторских объединений. Результаты проведения аудита предоставляются в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций для рассмотрения и принятия соответствующих мер». Данное изменение позволит повысить устойчивость безопасности информационной инфраструктуры.

В целом, проблемы обеспечения информационной безопасности приобретают особую чувствительность и остроту, требуя объективного и комплексного подхода к их решению. К ним, на основании проведенного исследования, отнесены:

- кадровый дефицит на IT-рынке;
- другим актуальным вопросом является несовершенство системы защиты персональных данных. Несмотря на повышенное внимание органов государственной власти к данной проблеме, вопрос утечки информации остается крайне острым;

- крайне чувствительным вопросом является несовершенство информатизации социальной работы. Обеспечение информационной безопасности в социальной сфере – одно из приоритетных направлений в деятельности органов государственной власти. Однако реализация деятельности по данному направлению сопряжена с рядом проблем, вызванных широким проникновением иностранных программ и приложений, преобладающими среди населения Российской Федерации, низким уровнем осведомленности граждан в области информационной безопасности;
- новые угрозы и вызовы обеспечения информационной безопасности в условиях усиливающейся геополитической напряженности. При этом важно учитывать не только внутренние, но и внешние факторы, новые угрозы и вызовы.

В условиях новых вызовов и угроз, усиления геополитической разбалансированности мира с учетом выявленных в рамках проведенного исследования проблем важно активизировать усилия в направлении совершенствования обеспечения информационной безопасности страны, в том числе уделить внимание следующим вопросам:

– защите объектов критической IT-инфраструктуры;
– совершенствованию механизмов обнаружения и предотвращения внешнего вредоносного воздействия на информационно-кибернетическое пространство;
– подготовке квалифицированных кадров в области цифровых технологий, информации и информационной безопасности.

Стоит учитывать, что разработка новых методов и средств защиты информационной безопасности сопряжена с угрозами сбора, накопления, хранения и обработки информации в информационных системах. В частности, данная проблема усиливается на фоне появления и развития новых средств и методов защиты, которая сопряжена с оценкой их качества и эффективности. Наряду с тем важно учитывать и разработку критериев, позволяющих оценить

их качество. Другим возможным направлением совершенствования в данной области послужит разработка и внедрение новых информационных технологий. При этом важно уделить особое внимание их защищенности. Целесообразность данного предложения объясняется тем, что совершенствование государственного и муниципального управления тесно сопряжено с необходимостью разработки новых концептуальных принципов построения функциональных узлов цифровой системы и организации взаимодействия данных узлов.

Данная проблема особенна актуальна для Тюменской области по причине циркуляции широкого объема информационных потоков. Однако стоит признать, что уровень научно-поисковых исследований в регионе в данном вопросе крайне низок. В данной связи следует уделить повышенное внимание данному вопросу.

Можно прийти к выводу, что еще направлением совершенствования обеспечения информационной безопасности послужит создание на региональном уровне целостной и многокомпонентной системы защищенного электронного документооборота с уклоном на электронную цифровую подпись. При разработке данного предложения стоит уделить внимание контролю целостности информации. В области совершенствования правовой политики в сфере информационной безопасности автор выпускной квалификационной работы, учитывая складывающиеся тенденции в информационно-кибернетическом пространстве обосновывает необходимость внесения изменения в действующий Федеральный закон путем дополнения его новыми статьями

Заключение

Настоящее исследование, посвященное изучению правовой политики в сфере обеспечения информационной безопасности, позволило сформулировать следующие выводы.

В результате рассмотрения теоретических и методологических основ информационной безопасности установлено, что в доктрине права не сложилось единого подхода к определению данного термина. Впрочем, несмотря на плюрализм мнений в данном вопросе нельзя отрицать, что в проанализированных подходах просматриваются общие черты. В частности, это выражается в понимании информационной безопасности как неотъемлемой составляющей национальной безопасности. Определение данного термина в указанном ключе отражает современные реалии – усиление геополитической напряженности, развернутой против Российской Федерации войны в информационной пространстве.

Проведение сравнительного исследования вопроса, связанного с информационной безопасностью сквозь призму исторической эпохи, позволило провести грань между определенным историческим периодом и настоящим временем.

В результате проведенного исследования установлено, что становление и развитие системы обеспечения информационной безопасности связывается с периодом развития древнерусского государства.

В настоящее время учитывая масштаб проникновения информационно-коммуникационных технологий в жизнь современного общества, органов государственной власти и экономических субъектов, а также высокий уровень зависимости создаваемых в Российской Федерации информационных систем от импортозамещения, на повестку дня особенно остро поставлен вопрос обеспечения информационной безопасности страны в условиях новых вызовов и угроз.

Последнее десятилетие в особенности обострило проблему усиления угроз в информационно-кибернетическом пространстве и использования информационных ресурсов для разрушения целостности информационной безопасности государства.

При этом важно учитывать, что истоки данной проблемы связываются и с отсутствием законодательной базы в сфере защиты кибернетического пространства, возрастанием напряженности между государствами в кибернетическом пространстве.

В результате рассмотрения информационной безопасности в структуре национальной безопасности представлено определение термина «национальная безопасность», рассмотрена её структура, определено место информационной безопасности в структуре национальной безопасности. Установлено, что национальные интересы государства и общества выступают фундаментальной основой информационной безопасности.

При этом уровень развития системы информационной безопасности Российской Федерации служит детерминантной развития национальной безопасности страны.

По результатам рассмотрения общих гарантий информационной безопасности, установлено, что импортозамещение в сфере информационной безопасности выступает одним из стратегических направлений, ориентированным на снижение зависимости от иностранных компонентов и оборудования, программного обеспечения, а также развитие отечественных IT-решений.

Данное направление принимает все новые очертания на фоне усиления геополитической напряженности, кибернетических угроз.

В эпоху глобализации развитые страны уделяют особое внимание обеспечению кибернетической безопасности, что выражается в инвестировании в создание и развитие системы национальных центров передового опыта области кибербезопасности.

В настоящее время в Российской Федерации принята и реализуется национальная программа «Цифровая экономика Российской Федерации», структуру которой образует шесть национальных проектов, в том числе «Информационная безопасность».

В целом показатели, предусмотренные в рамках реализации национального проекта ориентированы на минимизацию рисков утечек конфиденциальной информации, предотвращение возможных угроз и их последствий для национальной безопасности Российской Федерации.

В результате рассмотрения организационных гарантий информационной безопасности установлено, что во внутриполитической сфере деятельность органов государственной власти сосредоточена на предотвращении несанкционированного доступа и внешних вызовов, связанных с воздействием на функционирование информационной системы, а также обеспечение информационной безопасности в контексте каналов связи для выстраивания электронного взаимодействия территориальных органов государственной власти.

Деятельность органов государственной власти Российской Федерации в рамках внешнеполитического курса носит многогранный характер, поскольку не очерчивается исключительно повышением эффективности и сбалансированности развития IT-инфраструктуры, но и развивается в области обеспечения рационального использования информационных ресурсов.

Изучение вопроса, связанного с нормативными гарантиями информационной безопасности, позволило отметить Стратегию развития информационного общества, утвержденную указом Президента Российской Федерации от 09.05.2017 № 203 и рассчитанную на период 2017-2030 гг. В ней определены цели и коррелирующие ей задачи и меры по реализации внутренней и внешней политики государства в сфере применения информационно-коммуникационных технологий, направленных на информатизацию гражданского общества, обеспечение национальных

интересов и реализацию приоритетов признанных стратегически приоритетными.

По результатам рассмотрения проблем и определения перспектив обеспечения информационной безопасности сформулированы следующие выводы:

- в условиях новых вызовов и угроз, усиления геополитической разбалансированности мира с учетом выявленных в рамках проведенного исследования проблем важно активизировать усилия в направлении совершенствования обеспечения информационной безопасности страны, в том числе уделить внимание следующим вопросам: защите объектов критической IT-инфраструктуры, совершенствования механизмов обнаружения и предотвращения внешнего вредоносного воздействия на информационно-кибернетическое пространстве, а также подготовке квалифицированных кадров в области цифровых технологий, информации и информационной безопасности;
- кроме того, стоит учитывать, что разработка новых методов и средств защиты информационной безопасности сопряжена с угрозами сбора, накопления, хранения и обработки информации в информационных системах. В частности, данная проблема усиливается на фоне появления и развития новых средств и методов защиты, которая сопряжена с оценкой их качества и эффективности. Наряду с тем важно учитывать и разработку критериев, позволяющих оценить их качество;
- другим возможным направлением совершенствования в данной области послужит разработка и внедрение новых информационных технологий. При этом важно уделить особое внимание их защищенности.

Целесообразность данного предложения объясняется тем, что совершенствование государственного и муниципального управления тесно

сопряжено с необходимостью разработки новых концептуальных принципов построения функциональных узлов цифровой системы и организации взаимодействия данных узлов. Данная проблема особенна актуальна для Тюменской области по причине циркуляции широкого объема информационных потоков.

Однако стоит признать, что общий уровень научно-поисковых исследований в области рассмотрения проблем обеспечения информационной безопасности крайне низок. В данной связи следует уделить повышенное внимание проработке данного вопроса, что позволит более объективно подойти к обеспечению информационной безопасности.

Другим направлением совершенствования системы обеспечения информационной безопасности послужит создание на региональном уровне целостной и многокомпонентной системы защищенного электронного документооборота с уклоном на использование электронной цифровой подписи. При разработке данного предложения стоит уделить внимание контролю целостности информации.

В области правовой политики в сфере информационной безопасности следует уделить внимание вопросам повышения безопасности, хранения и обработки данных российских операторов персональных данных, которые в условиях геополитической напряженности приобретают крайнюю чувствительность. В данной связи в рамках правового поля целесообразно закрепить положение, связанное с установлением обязательной сертификации услуг в области облачного хранения и обработки персональных данных. Автор выпускной квалификационной работы обосновывает необходимость внесения изменений в Федеральный закон «О персональных данных» путем закрепления статьи 18.2 «Сертификация облачных сервисов». В рамках данной статьи предлагается закрепить следующее положение: «При сборе персональных данных оператор обязан использовать аккредитованные государством в соответствии с законодательством Российской Федерации облачные сервисы и технологии. Выдача сертификата осуществляется

органами исполнительной власти по согласованию с Федеральной службой безопасности Российской Федерации и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации».

Кроме того, для усиления информационной безопасности в динамично развивающемся информационно-кибернетическом пространстве следует поставить на повестку дня вопрос о внесении изменения в Федеральный закон «О персональных данных», направленного на своевременное выявление и устранение уязвимых мест в системе обработки персональных данных. В контексте предлагаемой новеллы автор выпускной квалификационной работы признает целесообразным расширить обязанности контролирующих органов путем закрепления в рамках правового поля проведения обязательного аудита внутренних процессов обработки данных. В данной связи обосновывается необходимость дополнения представленного Федерального закона ст. 19.1 «Аудит информационной безопасности», в рамках которой следует закрепить положение: «Операторы персональных данных обязаны ежегодно проводить независимый аудит системы обработки данных с привлечением к данному процессу аккредитованных профессиональных аудиторских объединений. Результаты проведения аудита предоставляются в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций для рассмотрения и принятия соответствующих мер». Данное изменение позволит повысить устойчивость безопасности информационной инфраструктуры.

Список используемой литературы и используемых источников

1. Александров И.Г. Информационные угрозы и информационная безопасность в современном мире // Региональные аспекты управления социально-экономическими процессами: материалы XV Всероссийской научно-практической конференции учащейся молодёжи, Чебоксары, 21 апреля 2022 года. Чебоксары: Издательско-полиграфическая компания «Новое время», 2022. С. 42-45.

2. Антонян Е.А. К вопросу о борьбе с современным экстремизмом и терроризмом в условиях использования новых технологий // Юридическое образование и наука. 2020. № 11. С. 13-16.

3. Байдак Е.С. Информационная безопасность как составляющая национальной безопасности // Наука. Инновации. будущее – 2023: сборник статей Международной научно-практической конференции, Петрозаводск, 12 декабря 2023 года. Петрозаводск: Международный центр научного партнерства «Новая Наука», 2023. С. 259-263.

4. Бирюков И.А. Проблемы импортозамещения программного обеспечения в России // Образование и наука без границ: социально-гуманитарные науки. 2023. № 21. С. 71-74.

5. Брюхомицкий Ю.А. Безопасность информационных технологий. В 2 ч. Ч. 1: учеб. пособие / Южный федер. ун-т; Ю.А. Брюхомицкий. Ростов-на-Дону: Изд-во ЮФУ, 2020. 173 с.

6. Будущее IT-сферы: что дает россиянам проект «Цифровые профессии». // Режим доступа: URL: https://национальныепроекты.рф/news/budushchee-it-sfery-chto-daet-rossiyanam-proekt-tsifrovye-professii/ (дата обращения: 27.06.2025).

7. Буряк В.В. Проблематика кибербезопасности в информационном обществе // Юридический факт. 2018. № 32. С. 25-31.

8. В первом полугодии 2024 года кратно выросло число атак на сферы телекоммуникации и строительства. // Режим доступа: URL:

https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-v-pervom-polugodii-2024-goda-zafiksirovan-kratnyj-rost-atak-na-sfery-telekoma-i-stroitelstva (дата обращения: 27.06.2025).

9. В Тюменской области продолжается переход на отечественное ПО в органах власти. // Режим доступа: URL: https://admtyumen.ru/ogv_ru/news/subj/more.htm?id=12103239@egNews (дата обращения: 08.05.2025).

10. Васюков В.Ф. Преступления в сфере высоких технологий и информационной безопасности: учебное пособие. М.: Прометей, 2023. 1086 с.

11. Грязнов С.А. Информационная безопасность организации // Modern Science. 2020. № 10-1. С. 50-53.

12. Егоров К.Н. Защита информации в России XX века // Актуальные проблемы защиты и безопасности: труды XXIV Всероссийской научно-практической конференции, Санкт-Петербург, 01-04 апреля 2021 года. Том 3. СПб: ФГБУ «Российской академии ракетных и артиллерийских наук», 2021. С. 457-463.

13. Жарова А.К. Информационное право. Правовое регулирование создания и использования информационной инфраструктуры: учебное пособие для вузов / А.К. Жарова. М.: Издательство Юрайт, 2024. 300 с.

14. Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации: учебное пособие. М.: Берлин: Директ-Медиа, 2015. 253 с.

15. Закон Российской Федерации от 05.03.1992 № 2446-1 «О безопасности» (утратил силу) // Российская газета. 1992. № 103.

16. Закон Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне» (ред. от 08.08.2024) // Собрание законодательства РФ. 1997. № 41. Стр. 8220-8235.

17. Зенков А.В. Информационная безопасность и защита информации: учебное пособие для вузов / А.В. Зенков. 2-е изд., перераб. и доп. М.: Издательство Юрайт, 2024. 107 с.

18. Зарипова Р.С., Мухаметзянов И.И. Роль импортозамещения в сфере информационной безопасности // ЕГИ. 2023. № 5 (49). С. 112-114.

19. Зарипова Р.С., Шакиров А.А. Проблемы обеспечения информационной безопасности больших данных // Информационные технологии в строительных, социальных и экономических системах. 2019. № 3-4 (17-18). С. 150-152.

20. Злыгостев Д.Д., Зарипова Р.С. Информационная безопасность как инструмент обеспечения экономической безопасности предприятий // Инновации в информационных технологиях, машиностроении и автотранспорте: сборник материалов Международной научно-практической конференции. 2017. С. 23-25.

21. ИБ в России и мире // Режим доступа: URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ib-v-rossii-i-mire/#:~:text=По%20оценке%20американского%20Центра%20стратегических,носителей%20информации%2C%20с%20различными%20целями. (дата обращения: 27.06.2025).

22. Инароков И.Р. Образование, структура и полномочия Всероссийской Чрезвычайной Комиссии по борьбе с контрреволюцией и саботажем // Моя профессиональная карьера. 2021. Т. 1. № 28. С. 28-33.

23. Искусство интеллекта: защита от хакерских атак усилится в разы // Режим доступа: URL: https://iz.ru/1683650/elizaveta-krylova/iskusstvo-intellekta-zashchita-ot-khakerskikh-atak-usilitsia-v-razy (дата обращения: 18.07.2025).

24. Как искусственный интеллект повышает кибербезопасность // Режим доступа: URL: https://www.rbc.ru/neweconomy/news/6554cc119a79477fa20d3dda (дата обращения: 18.07.2025).

25. Как поумнели камеры видеонаблюдения в Тюмени и области // Режим доступа: URL: https://72.ru/text/gorod/2024/01/13/73061624/ (дата обращения: 08.05.2025).

26. Канаев Д. DDoS-атака – основная угроза информационной безопасности // Режим доступа: URL: https://lib.itsec.ru/articles2/focus/ddos-ataka-osnovn-ugroza-informac-bezopasnosti (дата обращения: 18.07.2025).

27. Кенжетаев Б.Е. Информационная безопасность: понятие, сущность, содержание // Вестник Торайгыров университета. Гуманитарная серия. 2020. № 4. С. 36-45.

28. Килясханов И.Ш. Информационное право в терминах и понятиях: учеб. пособие / Ю.М. Саранчук; И.Ш. Килясханов. М.: ЮНИТИ-ДАНА, 2015. 136 с.

29. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Собрание законодательства РФ. 2014. № 31. Ст. 4398.

30. КНР – Закон о кибербезопасности принят. // Режим доступа: URL: https://www.imemo.ru/news/events/text/knr-zakon-o-kiberbezopasnosti-prinyat (дата обращения: 27.06.2025).

31. Кравченко Л.А., Субоч Д.В. Государственная политика информационной безопасности // Проблемы информационной безопасности социально-экономических систем: труды IX Международной научно-практической конференции, Гурзуф, 02-04 марта 2023 года / под редакцией О.В. Бойченко. Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2023. С. 40-41.

32. Кудакаев А.Р., Эшелиоглу Р.И. Криптографические методы защиты информации в современном мире // Современные технологии документооборота в бизнесе, производстве и управлении: сборник статей по материалам XXIII Всероссийской научно-практической конференции (с международным участием). Пенза, 2023. С. 105-108.

33. Ли С. Зарождение и развитие корпоративной культуры в компании «Лаборатория Касперского» // Экономика и социум. 2022. № 6-1 (97). С. 672-674.

34. Махмадов П.А. Информационная безопасность в системе политической коммуникации: состояние и приоритеты обеспечения (на материалах государств Центральной Азии): дисс... д-ра полит. наук. Душанбе, 2018. 323 с.

35. Озакман О.А. Применение систем искусственного интеллекта в защите информации // Актуальные исследования. 2025. № 27 (262). Ч. I. С. 28-31.

36. Органы власти Тюменской области переходят на централизованную IT-архитектуру. // Режим доступа: URL: https://www.osp.ru/resources/releases?rid=24403 (дата обращения: 08.05.2025).

37. Основные уроки информационной безопасности в 2024 году и прогнозы на будущее // Режим доступа: URL: https://infars.ru/blog/osnovnye-uroki-informatsionnoy-bezopasnosti-v-2024-godu-i-prognozy-na-budushchee/ (дата обращения: 27.06.2025).

38. Остапенко В.С. Информационная безопасность региональных органов исполнительной власти // Слово молодым ученым. 2009. № 1. С. 160-169.

39. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7) // Консультант плюс: справочно-правовая система.

40. Перекатова А.Д. Таинственные страницы истории: криптография вчера и сегодня // Вестник науки. 2019. № 7 (15). С. 37-50.

41. Петров Г.С. Информационная безопасность, как элемент национальной безопасности. Концептуальные подходы в современном мире // Высокотехнологичное право: генезис и перспективы: материалы III Международной межвузовской научно-практической конференции, Москва-Красноярск, 24-25 февраля 2022 года. Красноярск: Красноярский государственный аграрный университет, 2022. С. 196-201.

42. Подготовка топ-специалистов в сфере ИТ. // Режим доступа: URL: https://digital.gov.ru/activity/it-obrazovanie/podgotovka-top-speczialistov-v-sfere-it (дата обращения: 27.06.2025).

43. Постановление Лискинского районного суда Воронежской области от 29.07.2020 г. по делу № 1-189/2020 // Консультант плюс: справочно-правовая система.

44. Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // Российская газета. 2022. № 294.

45. Преступления против общественной безопасности и общественного порядка: учебник для вузов / ответственные редакторы А.В. Наумов, А.Г. Кибальник. 6-е изд., перераб. и доп. М.: Издательство Юрайт, 2025. 158 с.

46. Приговор Новочебоксарского городского суда Чувашской Республики от 21.12.2016 г. по делу № 1-318/2016 // Консультант плюс: справочно-правовая система.

47. Приговор Октябрьского городского суда Республики Башкортостан от 29.07.2020 г. по делу № 1-243/2020 // Консультант плюс: справочно-правовая система.

48. Приговор Саровского городского суда Нижегородской области от 15.02.2010 г. по делу № 1-14/10 // Консультант плюс: справочно-правовая система.

49. Приказ Федеральной службы по техническому и экспертному контролю от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета. 2013. № 136.

50. Распоряжение Правительства Тюменской области от 01.07.2013 № 1209-рп «Об утверждении Положения об информационной безопасности исполнительных органов государственной власти Тюменской области, подведомственных им учреждений» // Консультант плюс: справочно-правовая система.

51. Рассолов И.М. Информационное право: учебник и практикум для вузов / И.М. Рассолов. 7-е изд., перераб. и доп. М.: Издательство Юрайт, 2024. 427 с.

52. Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года. Режим доступа: URL: https://documents.un.org/doc/undoc/gen/n18/418/07/pdf/n1841807.pdf (дата обращения: 08.05.2025).

53. Рынок труда в России (ИТ и телеком). // Режим доступа: URL: https://www.tadviser.ru/index.php/Статья:Рынок_труда_в_России_(ИТ_и_телеком) (дата обращения: 27.06.2025).

54. Смирнов Ю.Н., Фатыхов Р.И. Об информационной безопасности промышленных предприятий в условиях цифровизации // Приборостроение и автоматизированный электропривод в топливно-энергетическом комплексе и жилищно-коммунальном хозяйстве. материалы IV Национальной научно-практической конференции. Казанский государственный энергетический университет. 2019. С. 43-46.

55. Соломатова Е.В. Исторические аспекты правового регулирования защиты конфиденциальной информации // Обеспечение безопасности личности, общества и государства в условиях глобализации: правовые и организационные проблемы и перспективы: сборник статей 52-й Всероссийской научно-практической конференции с международным участием студентов, магистров и молодых учёных, Ижевск, 25-26 апреля 2024 года. Ижевск: Удмуртский государственный университет, 2024. С. 437-446.

56. Столбов П.А. Состояние информационной безопасности в Российской Федерации // Вестник науки. 2024. № 6 (75). С. 1202-1208.

57. Точиева З.Ю. Национальные интересы Российской Федерации в информационной сфере и их обеспечение // Студенческий вестник. 2021. № 4-6 (149). С. 31-33.

58. Указ Президента Российской Федерации от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне» (ред. от 11.04.2024) // Собрание законодательства РФ. 1995. № 49. Ст. 4775.

59. Указ Президента Российской Федерации от 22.02.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» // Собрание законодательства РФ. 2015. № 21. Ст. 3092.

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

61. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации» // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

62. Указ Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // Собрание законодательства РФ. 2017. № 52. Ст. 8112.

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

64. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. 2021. № 27. Ст. 5351.

65. Управление доступом: развитие технологий, процессов, машинного обучения. URL: https://rt-solar.ru/events/blog/4080/ (дата обращения: 18.07.2025).

66. Федеральный закон от 20.12.1995 № 24-ФЗ «Об информации, информатизации и защите информации» (утратил силу) // Собрание законодательства РФ. 1995. № 8. Ст. 609.

67. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Собрание законодательства РФ. 2003. № 28. Ст. 2895.

68. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31. Ст. 3448.

69. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. № 31. Ст. 3451.

70. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» // Собрание законодательства РФ. 2011. № 1. Ст. 2.

71. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства РФ. 2011. № 15. Ст. 2036.

72. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2017. № 31. Ст. 4736.

73. Филонова А.А. Теоретические и исторические аспекты защиты информации в Российской Федерации // Вестник НИБ. 2022. № 45. С. 130-140.

74. Шахсуварова И.З. Информационная безопасность: теоретические основы понятия // Аллея науки. 2022. Т. 1. № 7 (70). С. 209-214.

75. Юлдашев Ю.Ж. Информационная безопасность в системе защиты национальных интересов Российской Федерации // Коммуникология: электронный научный журнал. 2020. Т. 5. № 2. С. 72-83.

76. InfoWatch: РФ заняла в 2024 году пятое место по числу утекших личных данных. URL: https://tass.ru/obschestvo/23439577 (дата обращения: 27.06.2025).

77. MarketsandMarkets: мировой рынок ИИ в кибербезопасности вырастет до 60,6 млрд долларов к 2028 году. URL:

https://cisoclub.ru/marketsandmarkets-mirovoj-rynok-ii-v-kiberbezopasnosti-vyrastet-do-60-6-mlrd-dollarov-k-2028-godu/ (дата обращения: 18.07.2025).