Тип работы: Дипломная работа

Предмет: Внешняя политика и дипломатия

1.2. Место информационной безопасности в системе национальной безопасности

На сегодняшний день информационная безопасность в российском законодательстве проявляется не только как самостоятельный вид безопасности, но и как аспект военного обеспечения национальной безопасности страны. Рассматриваемые новые вызовы и угрозы возникают в результате увеличения количества центров мирового экономического и политического развития, укрепления позиций глобальных и региональных стран-лидеров. В связи с этим информационная безопасность страны способствует дальнейшему повышению внутренней стабильности, наращиванию экономического, политического и военного потенциала, необходимого для укрепления ее роли как одного из влиятельных центров современного мира. В данном вопросе информационная безопасность представляется ключевой в условиях глубокой интеграции в информатизацию.
Законодательная власть РФ активно и оперативно реагирует на новые вызовы и угрозы национальной безопасности страны, например, два года назад был принят Федеральный закон «О внесении изменения в статью 330.1 Уголовного кодекса Российской Федерации» от 30.12.2020 № 525-ФЗ [55], также известный как «закон об иноагентах», который стал как никогда ранее актуален в условиях недавних и до сих пор продолжающихся масштабных беспрецедентных информационных атак на Российскую Федерацию. Важным в отношении обеспечения информационной безопасности выступает и Федеральный закон № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации», позволяющий правоохранителям четко определить действия по защите прав и свобод россиян, ограничить деятельность организаций, в том числе экстремистских, угрожающих национальной безопасности [53].
Таким образом, унификация федерального и регионального законодательства в сфере информационной безопасности и его формирование в соответствии с особенностями субъекта федерации при надлежащем соблюдении Федеральных законов – основная основа обеспечения информационной безопасности в РФ и неотъемлемая часть национальной безопасности в нашем государстве.
Качество, своевременность и достоверность информации определяют не только качество решений, которое принимают органы власти и управления, но процесс принятия самого решения. Информационные и психологические воздействия, осуществляемые через отдельные СМИ, создают атмосферу социальной напряженности, политическую нестабильность, вызывая конфликты между социальными, национальными, религиозными и массовыми беспорядками.

Основы информационной безопасности РФ предусматривают два классификатора национальных интересов в сфере информации [49]:
 продвижение на международной арене российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в области международной информационной безопасности;
 содействие созданию международно-правовых механизмов предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;
 организацию межведомственного взаимодействия при реализации государственной политики в области международной информационной безопасности.
Защита информационных ресурсов от несанкционированного доступа и обеспечение безопасности информационных и телекоммуникационных систем, развернутых и установленных в России [54, с. 1950] включает следующие задачи:
 повышение безопасности информационных систем, включая сети связи, в основном безопасность основных сетей связи и интегральных схем федеральных государственных учреждений, государственных учреждений субъектов Российской Федерации, финансового и банковского секторов, экономической деятельности, а также информационных систем и средств вооружения и военной техники оборудования, систем управления войсками и вооружением, экологически вредных и экономически важных отраслей промышленности; ускорить развитие отечественного производства аппаратного и программного обеспечения информационной безопасности и методов контроля его эффективности;
 обеспечение защиты информации, составляющей государственную тайну;
 расширение международного сотрудничества России в области разработки и безопасного использования информационных ресурсов для противодействия угрозе боевых действий в информационном поле.
Представляется, что решение вышеуказанных задач обеспечения безопасности страны возможно только путем создания интегрированной системы, совокупности законодательных актов и механизмов структурирования и взаимодействия, созданных на их основе для защиты интересов субъектов правоотношений. Устойчивость системы должна основываться на национальном консенсусе. Одним из основных компонентов системы национальной безопасности является информационная безопасность, которая выступает важным связующим звеном, связывающим все основные компоненты национальной политики в единое целое. В то же время очевидно, что роль информационной безопасности в системе национальной безопасности страны и ее место становятся все более важными. Это может произойти по следующим причинам:
 обеспечение национальных интересов во всех сферах национальной безопасности, угроз им и защита от этих угроз выражается и реализуется через информацию и информационные сферы;
 люди и их права, информация и информационные системы, а также права на них являются не только главной целью информационной безопасности, но и безопасностью во всех сферах;
 решение вопросов национальной безопасности связано с использованием информационных подходов как основного научного и практического метода;
 вопрос национальной безопасности носит ярко выраженный информационный характер [57, с. 37].
Таким образом, необходимо защитить информацию, в том числе так называемые технологические барьеры, используя системы управления доступом, антивирусных программ и других аппаратных средств и методов. Многие ученые считают, что информационная безопасность является совокупностью технических мероприятий по обеспечению безопасности. Информационная безопасность является важнейшим элементом обеспечения жизненно важных интересов государства, поскольку угрозы национальной безопасности страны во всех сферах деятельности страны все чаще осуществляются со стороны информационной среды, поэтому необходимо защищать информационные ресурсы, системы, их распространение и использование.

1.3 Международно-политическое взаимодействие с точки зрения обеспечения информационной безопасности

Взаимодействие государств в области информационной безопасности протекает в форме межгосударственного сотрудничества. Особое значение имеют заключение двусторонних и многосторонних договоров, взаимодействие государств в рамках международных организаций. В современном мироустройстве видится принципиальное значение взаимодействия в системе ООН. Комплексность и межотраслевой характер проблем информационной безопасности, вовлеченность различных сфер

правового регулирования остро проявляются в интеграционных объединениях. Европейская политика информационной безопасности имеет многоуровневую структуру с многосторонним участием, подразумевая совмещение прямого действия международных правовых норм с их имплементацией государствами - членами ЕС (многоуровневое регулирование). Нынешняя ситуация усугубляется тем фактом, что информационно-коммуникационные технологии в настоящее время задействованы во всех сферах человеческого существования и общества. В этой связи особой проблемой является сложность комплексного межведомственного регулирования.

Количество вреда, постоянно причиняемого в сфере информации и коммуникаций, растет. Например, по данным Европейской комиссии ЕС, 100 миллионов человек ежедневно становятся жертвами киберпреступности, а общий глобальный ущерб, причиняемый киберпреступностью, оценивается более чем в 44 000 миллиардов долларов в год. Быстрое развитие технологий часто превосходит их теоретическое и общее понимание.

Европейская политика информационной безопасности имеет многоуровневую структуру с многосторонним участием, подразумевающую сочетание прямого действия международно-правовых норм и имплементации государствами-членами ЕС (многоуровневое регулирование). Как государственные, так и частные субъекты играют важную роль в системе информационной безопасности ЕС.

Главным препятствием, которое подрывает усилия ЕС в области информационной безопасности, является то, что этот вопрос прямо не освещен в его учредительном договоре. «Принцип авторизации» (Principal of Awarding) оставляет ЕС возможность рассмотреть вопрос информационной безопасности в качестве одного из своих возможностей в других областях [20, с. 44].

Серьезной проблемой является поиск правовой основы возможностей ЕС в области информационной безопасности во внешних отношениях. Сам потенциал считается неизбежным в связи с угрозой кибератак и киберпреступности на инфраструктуру самого Союза, а также с возможностью трансграничного ущерба от таких действий, направленных против одного из его членов. Например, Европейская комиссия отметила, что, поскольку киберпреступность как ключевой элемент проблем информационной безопасности по своей сути является транснациональной, необходимы соответствующие международные соглашения, поднимающие вопрос о юрисдикции в соответствии с международным правом.

На семинаре Регионального форума АСЕАН по мерам кибербезопасности и их правовым и культурным аспектам, состоявшемся в Пекине в 2013 году, политико-правовой подход государства в современных условиях, как сильные, так и слабые страны обеспокоены потенциальной уязвимостью легитимности административных систем в киберпространстве. В этой связи важным первым шагом в разработке правил обеспечения информационной безопасности является политическое соглашение, достигнутое в 2013-2016 годах между 15 государствами. Группа правительственных экспертов ООН по международной информационной безопасности заявила, что государствам не следует использовать посредников для совершения международно незаконных действий в киберпространстве.

Действия Организации Объединенных Наций в области информационной безопасности весьма фрагментированы, и экспертный анализ проблемы «разбросан» по сложным системам органов разного уровня Сотрудничество учреждений и структурных подразделений ООН в настоящее время является важным условием дальнейшего развития совместных действий государств и принятия международных норм [37, с. 5].

Предпосылками для создания гарантий информационной безопасности интеграционных и картельных объединений являются политическая и экономическая зависимость вовлеченных государств. Ярким примером является сотрудничество стран Азиатско-Тихоокеанского региона. Это происходит в условиях непрерывной геополитической конкуренции, политических, экономических и социокультурных различий. Стремление к региональной безопасности и стабильности определило задачу создания общей информационно-коммуникационной инфраструктуры, которая снижает риск дестабилизации взаимозависимых цифровых систем и способствует получению крупных региональных и национальных социально-экономических выгод. Это привело к активному национальному взаимодействию в рамках Ассоциации государств Юго-Восточной Азии (АСЕАН) и Азиатско-Тихоокеанского экономического сотрудничества (АТЭС). Необходимость предотвращения и смягчения последствий злонамеренного использования Интернета в преступных и террористических целях должна была стимулировать обмен информацией между национальными правоохранительными органами и установление региональных стандартов внутреннего законодательства и политики. Тем не менее, сотрудничество между государствами сталкивается с вопросом суверенитета в политико-правовом регулировании отношений в киберпространстве при желании государств использовать киберпространство в национальных целях.

Несмотря на усилия региональных политических форумов и многочисленные политические декларации, существует тенденция отдавать приоритет национальной внутренней информационной безопасности. Это приводит к его растущей милитаризации.
Во-первых, существуют различия в понимании того, как принципы международного права должны применяться к формированию средств защиты и стабилизации киберпространства. Во-вторых, цифровая инфраструктура развивается очень (на удивление) быстро, поэтому правительства и общественные системы очень зависят от нее. В-третьих, признание киберпространства «5-м полем военных действий». Его враждебное и злонамеренное использование потенциально может привести к обострению существующих конфликтов.
Неопределенность в структуре регулирования лишает региональные политические форумы способности государства участвовать в коллективных действиях. Страна не находит сильной политической мотивации для формирования строгих норм, но неопределенность предлагает стратегическое и тактическое использование потенциала киберпространства для своих геополитических целей - национальных интересов.
Особенность правового регулирования информационной безопасности в Евразийском экономическом союзе связана с происходящими процессами цифровой трансформации. Обращаясь к положениям стратегического документа Высшего Евразийского экономического совета от 11.10.2017 № 12 «Основные направления реализации цифровой повестки Евразийского экономического союза до 2025 года» [36], необходимо отметить, что «государства - члены ЕАЭС в своих стратегиях и программах (на национальном уровне) развития экономик активно решают ряд задач по выработке ответа вызовам цифровой трансформации экономики». Деятельность стран Евразийского экономического союза в сфере обеспечения информационной безопасности, реализуется активно, о чем свидетельствует работа по комплексной защите информации в рамках функционирования единой интегрированной системы Союза. Так, в целях унификации подходов к обеспечению информационной безопасности Коллегией ЕЭК разработаны перечень стандартов и рекомендаций, применяемые при защите веб-сервисов, защиты информации с использованием средств криптографической защиты, электронной цифровой подписи, сервисов доверенной третьей стороны. В финансовой системе ЕАЭС успешно разрешены некоторые вопросы обеспечения информационной безопасности, например, сложились единые стандартизированные подходы по регулированию вопросов кибербезопасности в финансовой сфере, киберустойчивости и надзору за возможными угрозами и рисками.
Кроме этого, Концепция общего финансового рынка Евразийского экономического союза установила положение о том, что в случае выявления угроз информационной безопасности финансовые регуляторы направляют в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России уведомления, содержащие общие характеристики и основные параметры компьютерных атак [3].
Одной из приоритетных задач обеспечения информационной безопасности на евразийском пространстве является внедрение современных систем идентификации, включая нейросети, технологии распознавания лиц. Предполагается, что данная задача найдет активное применение в таможенной сфере. В этой связи особое значение заслуживают положения Стратегии развития таможенной службы до 2030 года. Для реализации сформулированной задачи необходим действенный усовершенствованный механизм эффективного противодействия угрозам национальной безопасности, в том числе информационной.
Отметим, что целый ряд направлений по цифровизации таможенной сферы обозначен в Плане мероприятий на период 2021-2024 гг. по реализации Стратегии развития таможенной службы Российской Федерации до 2030 года, утвержденном Министерством финансов РФ и Правительством РФ, но отдельно (например, в виде раздела) вопросы правового регулирования исследуемого направления в указанном плане не освещены.
Для развития современных информационных технологий, отечественной информационной индустрии, включая ИТ, для удовлетворения потребностей внутреннего рынка, его продуктов и выпуска этих продуктов на мировом рынке, а также для обеспечения накопления, сохранения и эффективного использования внутренних информационных ресурсов [1, с. 19].
Крайняя уязвимость информационно-коммуникационных технологий остро ставит вопросы безопасности общественных отношений, которые складываются в связи с ними. Наибольшая озабоченность связана с безопасностью систем автоматического управления производственными и технологическими процессами государственной инфраструктуры, а также гражданской безопасностью (идентификация, медицинское обслуживание и т.д.). Информационная безопасность (кибербезопасность), которая лежит в ее основе,

также важна при использовании информационно-коммуникационных технологий в военных операциях. Кибершпионаж, кибертерроризм и киберпреступность основаны на их нарушениях. В природе проблем информационной безопасности присутствует трансграничный элемент.
Таким образом, на сегодняшний день реализация государственной суверенности в области информационной безопасности получила наибольший рост в результате формирования международного правового института международной информационной безопасности. Государству следует осуществлять и сознательно оказывать содействие в осуществлении любой деятельности по развитию безопасности информационных систем. Широкий спектр проблем и угроз информационной безопасности в современных условиях требует дальнейшего развития интеграционного сотрудничества для противодействия глобальным вызовам цифровой трансформации и обеспечения качественного и устойчивого экономического роста государств - участников Евразийского экономического союза в целях ускоренного перехода экономик на новый технологический уклад, формирования новых индустрий и рынков, развития трудовых ресурсов, синхронизации цифровых инноваций. В данном контексте речь идет уже не только о применении информационно-коммуникационных технологий, а предполагается использование новых бизнес-процессов, цифровых моделей. Что предполагает развитие и совершенствование организационно-методических основ обеспечения информационной безопасности интеграционных объединений.

1. Алексеев М. Д. Угрозы обеспечения экономической безопасности РФ / М. Д. Алексеев // Вестник НИЦ МИСИ : актуальные вопросы современной науки. – 2018. – № 5. – С. 18-26.
2. Бабаш, А. В. Информационная безопасность. Лабораторный практикум : Учебное пособие / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – Москва : КноРус, 2016. – 136 с.
3. Банк России завершил объединение финансовых регуляторов стран ЕАЭС в области взаимодействия по вопросам информационной безопасности – Текст : электронный // ЦБ РФ.ru : [сайт]. – 2018. – 15 нояб. – URL: https://cbr.ru/Press/event/?id=2231 (дата обращения: 26.04.2023)
4. Барт, А. А. Сущность и структура механизма экономической безопасности / А. А. Барт // Современные тенденции в экономике и управлении: Новый взгляд. – 2019. – 499 с.
5. Богомолов, В. А. Экономическая безопасность : учебное пособие для студентов вузов, обучающихся по специальностям экономики и управления / В. А. Богомолов. – Москва, 2020. – 295 с.
6. Буравилина, Ю. И. Обострение проблемы экономической безопасности в условиях геополитического кризиса и санкционного давления западных стран / Ю. И. Буравилина, А. А. Сенчило // Экономика и бизнес: теория и практика. – 2016. – № 11. – С. 15-17.
7. Василькова, В. Д. Проблемы экономической безопасности компаний в современных условиях / В. Д. Василькова, Е. Г. Марамыгина // Новая наука: Современное состояние и пути развития. – 2016. – № 12-1. – С. 75-77.
8. Галимуллина, Н. А. Подходы к анализу экономической безопасности региона / Н. А. Галимуллина // Актуальные проблемы права и государства в XXI веке. – 2017. – № -3. – С. 177-181.
9. Гафнер, В. В. Информационная безопасность : Учебное пособие / В.В. Гафнер. – Ростов-на-Дону: Феникс, 2017. – 324 с.
10. Громов, Ю. Ю. Информационная безопасность и защита информации : Учебное пособие / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. – Старый Оскол : ТНТ, 2017. – 384 с.
11. Дубень, А.К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению // Международное право и международные организации – Текст : электронный // сайт. – 2022. – № 1. – URL: https; //nbpubMLcomlbmy_read_artide.php?id=37490 (дата обращения: 26.04.2023)
12. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт : Монография / Л. Л. Ефимова, С. А. Кочерга. – Москва: ЮНИТИ-ДАНА, 2016. – 239 с.
13. Ефимова, Л. Л. Информационная безопасность детей. Российский и зарубежный опыт : Монография / Л. Л. Ефимова, С. А. Кочерга. – Москва: ЮНИТИ, 2016. – 239 с.
14. Жариков, Р. В. Комплексный анализ в оценке рисков экономической безопасности / Р. В. Жариков // Конкурентоспособность в глобальном мире: экономика, наука, технологии. – 2017. – № 11. – С. 1436-1437.
15. Запечников, С. В. Информационная безопасность открытых систем. В 2-х т. Т.1 – Угрозы, уязвимости, атаки и подходы к защите / С. В. Запечников, Н. Г Милославская. – Москва: ГЛТ, 2017. – 536 с.
16. Запечников, С. В. Информационная безопасность открытых систем. В 2-х т. Т.2 – Средства защиты в сетях / С. В. Запечников, Н. Г. Милославская, А. И. Толстой, Д. В. Ушаков. – Москва : ГЛТ, 2018. — 558 с.
17. Земскова, Е. С. Инновационная безопасность как подсистема экономической безопасности / Е. С.

Земскова // Контентус. – 2019. – № 3 (80). – С. 65-72.
18. Ильенкова, Н. Д. Этапы программы анализа рисков и экономической безопасности / Н. Д. Ильенкова // Сб. ст.: Анализ и современные информационные технологии в обеспечении экономической безопасности бизнеса и государства Сборник научных трудов и результатов совместных научно-исследовательских проектов. РЭУ им. Г. В. Плеханова. – Москва : Аудитор, 2016. – с. 171-175.
19. Ищук, Я. Г. Состояние киберпреступности граждан в контексте обеспечение защиты их основных прав и свобод // Обеспечение прав и свобод человека в деятельности правоохранительных органов: сборник статей / под науч. ред. докт. юрид. наук А. Я. Грищко. Рязанский филиал МосУ МВД России им. В. Я. Кикотя, 2018. – С. 37–42.
20. Капустин, А. Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности / А. Я. Капустин // Журнал зарубежного законодательства и сравнительного правоведения. 2017. – № 6. – С. 44-51.
21. Карцхия, А. А. Кибербезопасность и интеллектуальная собственность / А. А. Карцхия // Вопросы кибербезопасности. – 2018. – №1 (2). – 63 с.
22. Комитет ООН принял российский проект резолюции в сфере информационной безопасности [Электронный ресурс] URL : https://m.realnoevremya.ru/news/264922-oon-prinyala-rossiyskiy-proekt-rezolyucii-v-sfere-informacionnoy-bezopasnosti (дата обращения: 26.04.2023)
23. Кулешов, В. М., Тарасенко, А. А. Международная информационная безопасность как вектор развития национальной безопасности России и Германии / В. М. Кулешов, А. А. Тарасенко // Социально-экономические явления и процессы. – 2019. – Т. 14. – № 105. – С. 60-73.
24. Куява, Т. Ю. Киберпреступность: проблемы уголовно-правовой оценки и организации противодействия / Т. Ю. Куява // Молодой ученый. – 2016. – №29. – С. 255-257.
25. Ложкова, Ю. Н. Информационный менеджмент : учебное пособие для бакалавров по направлению обучения 38.03.05 «Бизнес-информатика» / Ю.Н. Ложкова ; Алт. гос. техн. ун-т, БТИ. – Бийск: Изд-во Алт. гос. техн. ун-та, 2016. – 139 с.
26. Малюк, А. А. Информационная безопасность : концептуальные и методологические основы защиты информации / А.А. Малюк. – Москва : ГЛТ, 2016. – 280 с.
27. Международная информационная безопасность в двусторонних отношениях России и США [Электронный ресурс]. URL: https://ai-news.ru/2023/02/mezhdunarodnaya_informacionnaya_bezopasnost_v_dvustoronnih_otnosheniya.html (дата обращения: 26.04.2023)
28. Номоконов, В. А. Актуальные проблемы борьбы с киберпреступностью / В. А. Номконов // Компьютерная преступность и кибертерроризм : сборник научных работ. 2018. – №. 1. – С. 77-79.
29. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года [Электронный ресурс]. URL: https://www.garant.ru/products/ipo/prime/doc/70541072/ (дата обращения: 26.04.2023)
30. Партыка, Т. Л. Информационная безопасность : Учебное пособие / Т.Л. Партыка, И.И. Попов. – Москва : Форум, 2016. – 432 с.
31. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. – Москва : АРТА, 2016. – 296 с.
32. Резолюция A/K.E8/73/27 от 5 декабря 2018 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Электронный ресурс]. URL: https://www.hse.ru/data/2023/02/06/2044873314/Рез%205%2012%2018.pdf(дата обращения: 26.04.2023)
33. Резолюция A/КБ8/73/264 от 22 декабря 2018 г. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности»[Электронный ресурс]URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/04/PDF/N1846504.pdf?OpenElement (дата обращения: 26.04.2023)
34. Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» [Электронный ресурс]. URL: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/a_res_53_70.pdf (дата обращения: 26.04.2023)
35. Резолюция, принятая Генеральной Ассамблеей ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий» [Электронный ресурс] URL: https://namib.online/wp-content/uploads/2023/02/A.RES_.76.19.pdf (дата обращения: 26.04.2023)
36. Решение Высшего Евразийского экономического совета от 11.10.2017 № 12 «Основные направления

реализации цифровой повестки Евразийского экономического союза до 2025 года» [Электронный ресурс] URL: https://docs.cntd.ru/document/555625953 (дата обращения: 26.04.2023)
37. Ромашкина, Н. П. Глобальные военно-политические проблемы международной информационной безопасности : тенденции, угрозы, перспективы / Н. П. Ромашкина // Вопросы кибер-безопасности. – 2019. – № 1(29). – С. 2-9.
38. Россия и США создадут рабочую группу по кибербезопасности, заявил Путин [Электронный ресурс]. URL: https://ria.ru/20170708/1498143045.html (дата обращения: 26.04.2023)
39. Семененко, В. А. Информационная безопасность : Учебное пособие / В.А. Семененко. — Москва : МГИУ, 2017. – 277 с.
40. Сергей Лавров обозначил контуры внешней политики Российской Федерации [Электронный ресурс]. URL: https://katyusha.org/obshhee-delo/sergej-lavrov-oboznachil-konturyi-vneshnej-politiki-nakanune-obrashheniya-prezidenta-k-federalnomu-sobraniyu.html (дата обращения: 26.04.2023)
41. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. – 4-е изд. – Москва : Флинта, 2016. – 224 с.
42. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков. – Брянск: Брянский государственный технический университет, 2012.– 224 с.
43. Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/1479(дата обращения: 26.04.2023)
44. США обвинили Россию в кибератаках на Демпартию [Электронный ресурс]. URL: https://www.rbc.ru/politics/07/10/2016/57f7ff559a7947d68959e530 (дата обращения: 26.04.2023)
45. Тулегенов, В. В. Киберпреступность как форма выражения криминального профессионализма / В. В. Тулегенов // Криминология: вчера, сегодня, завтра. – 2014. – № 2 (33). – С. 94– 97.
46. Указ Президента Российской Федерации от 17.03.2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» [Электронный ресурс] URL: http://www.kremlin.ru/acts/bank/27040 (дата обращения: 26.04.2023)
47. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 26.04.2023)
48. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_216363/ (дата обращения: 26.04.2023)
49. Указ Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» [Электронный ресурс] URL: https://www.garant.ru/products/ipo/prime/doc/400473497/
50. Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [Электронный ресурс] URL: http://publication.pravo.gov.ru/Document/View/0001202205010023
51. Указ Президента РФ от 31 марта 2023 г. № 229 «Об утверждении Концепции внешней политики Российской Федерации»[Электронный ресурс] URL: https://www.garant.ru/products/ipo/prime/doc/406543869/ (дата обращения: 26.04.2023)
52. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] Режим доступа: Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»
53. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации от 31.07.2017 г. №31 (часть I) ст. 4736
54. Федеральный закон от 28 декабря 2012 г. № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» // Собрание законодательства Российской Федерации от 31 декабря 2012 г. N 53 (часть I) ст. 7597
55. Федеральный закон от 30 декабря 2020 г. № 525-ФЗ «О внесении изменения в статью 330.1 Уголовного кодекса Российской Федерации» // Собрании законодательства Российской Федерации от 4 января 2021 г. N 1 (часть I) ст. 64
56. Хадисов, М. Р. Интегральная оценка уровня экономической безопасности региона при сравнительном

анализе / М. Р. Хадисов // Вестник экономической безопасности. – 2015. – № 4. – С. 71-78.
57. Чек-лист взаимодействия операторов персональных данных с ГосСОПКА [Электронный ресурс] URL: https://www.itsec.ru/articles/chek-list-vzaimodejstviya-operatorov-personalnyh-dannyh-s-gossopka (дата обращения: 26.04.2023)
58. Чекунов, И. Г. Киберпреступность: понятие и классификация / И.Г. Чекунов // Российский следователь. – 2018. – № 2. – С. 37 - 44.
59. Чекунов, И. Г. Современные киберугрозы : уголовно–правовая и криминологическая классификация и квалификация киберпреступлений / И. Г. Чекунов // Право и кибербезопасность. – 2017. – С. 9 - 22.
60. Чернова, В. В. Экономическая безопасность РФ: проблемы и пути решения / В. В. Чернова // Вестник научных конференций. – 2015. – № 1-1. – С. 157-159.
61. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. – Москва : Гелиос АРВ, 2017. – 336 с.
62. Экономическая безопасность : учебник и практикум для бакалавриата и магистратуры / отв. ред. Ю. Д. Романова. – Москва : Издательство Юрайт, 2019. – 495 с.
63. Oxford English Dictionary [Электронный ресурс] // URL: http:/ /www. askoxford.com/ (дата обращения: 21.03.2023).