Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт
институт
Кафедра международного права
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т.Ю. Сидорова
подпись инициалы, фамилия
« _____» _____ 2022г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01.01 Международное и иностранное право
код – наименование направления

Обеспечение информационной безопасности в сети Интернет: сравнительно – правовой анализ
тема

Руководитель _____ к.ю.н., доцент В.В. Терешкова
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ М.Д. Чеконов
подпись, дата инициалы, фамилия

Красноярск 2022

СОДЕРЖАНИЕ

Введение

Сегодня проблема обеспечения информационной безопасности считается необходимый элементом обороноспособности любой страны. Данная необходимость вызвана стремительным развитием информационных и компьютерных технологий, а также увеличением количество противоправных действий, совершаемых в информационной среде. Кроме того, высокие темпы развития способствовали ускорению процесса политизация данной сферы. 20 мая 2022 года Президент РФ В.В. Путин отметил возрастающее число атак на российскую информационную структуру, отметив что «против России развязана настоящая агрессия, война в информационном пространстве»[1].

Использование информационного пространства как политического инструмента представляет собой угрозу для любой страны. В связи с этим ведется активное, а местами и открытое противостояние за получения доминирующего положения в информационном пространстве, что придает проблеме обеспечения информационной безопасности не только чисто технический или законодательный характер, но и политический.

Стремительный рост количества угроз информационной безопасности и недостаточное урегулирование данной области вызывают изменения подходов различных стран и международных организаций к изучаемой тематике. Обеспечение информационной безопасности стоит на повестке дня у всего мирового сообщества в целом. Эффективное функционирование международных институтов является гарантом обеспечения надежной и справедливой системы информационной безопасности. Вооруженные кризисы и их последствия ставят перед государствами новые вызовы в области обеспечения информационной безопасности.

[1]Заседание Совета безопасности РФ от 20 мая 2022 года // Совет Безопасности Российской Федерации. Официальный сайт. – 2022. – URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения: 20.05.2022).

Институт информационной безопасности является одной из наиболее распространенных тем для исследования. Начиная с 00-ых годов, количество работ в данной области увеличивается. За теоретическую основу были взяты труды таких авторов как А.В. Зенков, В.В. Гафнер, В.Ф. Шаньгин, В.И. Яснев, А.В. Дорожкин, А.Л. Сочков, О.В. Яснев, Е.В. Вастрецова.

Авторами исследуются отдельные аспекты информационной безопасности, ее история или формы реализации. Как правило такие работы не отображают многосторонность изучаемого вопроса и его взаимосвязь с другими институтами права. Однако комплексного исследования информационной безопасности не проводилось

Объектом данного исследования служат отношения по обеспечению информационной безопасности. Предмет данного исследования - подходы к регулированию и обеспечению информационной безопасности в Российской Федерации, других странах и международных организациях.

Цель настоящей работы заключается в исследовании нормативно – правовой регламентации в области обеспечения информационной безопасности. Для достижения указанной цели были поставлены следующие задачи:

- Раскрыть понятие «Информационная безопасность» и определить ее сущность
- Проанализировать принципы информационной безопасности
- Раскрыть понятие «Угроза информационной безопасности»
- Определить существующие виды угроз информационной безопасности
- Произвести анализ мер, направленных по обеспечение информационной безопасности
- Определить перспективные направления и проблемы развития обеспечения информационной безопасности

Методологическая основа работы включает в себя такие методы, как системный анализ, обобщение, сравнение и типологизацию.

Эмпирическую основу исследования составили национальные, зарубежные и международные правовые акты, в том числе межгосударственные соглашения, решения международных организаций, национальные и зарубежные судебные решения, стратегические документы, проекты международных документов и документы технического характера.

Выпуская квалификационная работа содержит следующую структуру: введение, две главы, заключение, список использованных источников.

Глава 1. Правовая регламентация информационной безопасности.

1.1. Правовое регулирования информационной безопасности.

С древнейших времен наблюдается использование различных механизмов защиты информации, так, например, известно, что ещё в Древнем Египте и Древнем Риме применялся такой способ кодирования информации как тайнопись. Г.П. Жигулин отмечает следующее: «По свидетельству Геродота, уже в V в. до н. э. применялось кодирование информации. Классическим примером одного из первых применений криптографии является так называемый шифр „Цезаря“»[2].

Таким образом, зарождение концепции информационной безопасности прослеживается еще задолго до XX века, однако, согласно современной трактовке, понятие «информационная безопасности» тесно связано с развитием информационных и компьютерных технологий во второй половине XX века.

Правовое регулирование информационной безопасности и деятельности по ее обеспечению носит комплексный характер, главной особенностью которого является разделение правовых актов на международные и национальные. Национальное законодательство в свою очередь также подразделяется на три большие группы – стратегические документы, законодательные акты и подзаконные акты.

Первым стратегическим документом РФ в области информационной безопасности является Доктрина информационной безопасности[3], принятая в 2000 году. В 2016 году, данный документ утратил силу году связи с

[2]Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности. Санкт-Петербург: СПбНИУИТМО, 2014. С 8.

[3]Доктрина информационной безопасности Российской Федерации : указ Президента РФ от 09.09.2000 N ПР-1895) // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru/ (дата обращения: 01.01.2022).

утверждением новой Доктрины информационной безопасности Российской Федерации[4].

М.И Яхъева, анализируя данные доктрины, выделяет четыре фундаментальных тезиса, составляющих суть национальных интересов в области информационных правоотношений. К ним относятся:

1. «Гарантированность прав и свобод человека в области получения информации и пользования ею, обеспечение интеллектуального и духовного развития России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурных и научных возможностей нашего государства;
2. Осуществление информационного сопровождения как внутренней, так и внешней государственной политики страны;
3. Поступательное развитие информационных технологий в соответствии с последними достижениями в сфере «digital»;
4. Создание комплексной системы защиты информационных ресурсов; как тех которые уже функционируют на территории РФ, так и тех, которые планировались создаваться в долгосрочной перспективе»[5].

Сравнительный анализ данных стратегических документов Российской Федерации позволяет сделать вывод, что в Доктрине информационной безопасности РФ 2016 г., в отличие от предыдущей Доктрины, акцент смещен на стратегическое планирования политики государства, касательно обеспечения информационной безопасности как неотъемлемого элемента национальной безопасности России.

А. Н. Мещерякова, анализируя данное изменения пишет следующее: «Еще одним не менее важным нововведением Доктрины информационной безопасности РФ 2016 года являются усовершенствованные задачи

[4]Доктрина информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 N 646 // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru/ (дата обращения: 12.02.2022).
[5]Яхъева М. И. Информационная безопасность как составная часть национальной безопасности РФ. 2020. С. 43.

государственных органов в рамках деятельности по формированию и усовершенствованию системы обеспечения информационной безопасности»[6].

Стремительное увеличение количества угроз информационной безопасности в Доктрине 2016 значительное внимание уделяется такому вопросу как обеспечение критической информационной инфраструктуры, подчеркивая важность обеспечения бесперебойного и устойчивого ее функционирования. В документе также отмечается важность обеспечения защиты частной жизни граждан при обработки принадлежащих им персональных данных. Эффективная защита информационных систем, посредством которых осуществляется обработка персональных данных граждан, является одним из наиболее важных аспектов современной информационной безопасности.

В рамках реализации Доктрины информационной безопасности 2016г. были приняты соответствующие федеральные законы. Так для обеспечения правовой регламентации противодействия компьютерным атакам в 2017 г. был принят Федеральный закон «О безопасности критической информационной структуры Российской Федерации»[7].

В целях проверки на достоверность сведений и материалов, размещенных в сети «Интернет», в том же 2017 году принимается Федеральный закон «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”», закрепляющий качественные изменения в регулировании информационно-телекоммуникационных сетей и информационных средств, с помощью которых осуществляется прямой доступ к ограниченным на территории РФ ресурсам и сетям.

Доктрина информационной безопасности Российской Федерации от 2016 года существенно расширяет круг общественных отношений, попадающих под государственное регулирование.

---

[6]Мещерякова А. Н. «Сравнение Доктрин ИБ РФ 2000 года и 2016 года». // НвсФ ФГУП «НТЦ «Атлас» - [Электронный ресурс] – Режим доступа: https://www.atlasnsk.ru/news/186/ (дата обращения:: 12.04.2022).

[7]О безопасности критической информационной инфраструктуры Российской Федерации : федеральный закон от 26.07.2017 N 187-ФЗ // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru/ (дата обращения: 04.03.2022).

Отметим, что информационная безопасность является не только самостоятельным, отдельным видом безопасности, но и важным аспектом военного обеспечения национальной безопасности Российской Федерации. В Стратегии национальной безопасности Российской Федерации от 2021 г.[8] информационная безопасность отмечается как важнейший элемент национальной безопасности. Согласно данной стратегии одной из приоритетных задач в области обеспечения информационной безопасности является «укрепление и совершенствования информационной инфраструктуры в Вооруженных Сил, других войск, воинских формирований и органов, а также разработчиков и изготовителей вооружения, военной и специальной техники»[9].

Министерством Обороны Российской Федерации отмечено, что «в числе главных направлений совершенствования системы обеспечения информационной безопасности в области обороны отнесены:

- Стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;
- Совершенствование системы обеспечения информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;
- Прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам в информационной сфере»[10].

В Российской Федерации с 1995 г. по 2006 г. основополагающим законодательным актом, регулирующим общественные отношения в информационной сфере, являлся Федеральный закон РФ «Об информации,

[8]Стратегия национальной безопасности Российской Федерации : указ Президента от 02.07.20221 № 400 // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 01.01.2022).
[9]Там же.
[10] Концептуальные взгляды на деятельность Вооружённых Сил в информационном пространстве // Официальный интернет-портал правовой информации http://www.pravo.gov.ru (дата обращения: 20.04.2022).

информатизации и защите информации»[11], положения которого были направлены «на регулирование в области формирования и использования информационных ресурсов, создание и использовании информационных технологий, защиты информации» (ст. 1)[12]. Обеспечение национальной безопасности в информационной среде было закреплено данным законом как одно главных направлений развития государственной политики.

В 2006 г. был принят Федеральный закон РФ «Об информации, информационных технологиях и защите информации»[13]. Г.П. Жигулин отмечает, что закон «существенно дополнил правовую базу отмененного закона и до сих пор остается основополагающим нормативным правовым актом в информационной сфере»[14].

Федеральный закон «О безопасности»[15] играет важную роль в обеспечении информационной безопасности, так как в нем закреплены основные принципы и направления деятельности РФ по обеспечению всех видов безопасности, включая информационную. Наряду с этим, определен четкий перечень полномочий органов государственной власти и местного самоуправления, необходимых для обеспечения информационной безопасности, а также статус Совета Безопасности Российской Федерации.

В целях обеспечения безопасности при работе с персональными данными, в РФ действует ФЗ «О персональных данных»[16] от 27.06.2006 года, определяющий процедуры получения, хранения, использования, удаления и передачи персональных данных. В настоящее время в Государственной Думе

[11]Об информации, информатизации и защите информации : федеральный закон от 20.02.1995 N 24-ФЗ // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 12.02.2022).
[12]Об информации, информатизации и защите информации : федеральный закон от 20.02.1995 N 24-ФЗ // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 12.02.2022).
[13] Об информации, информационных технологиях и о защите информации : федеральный закон от 27.07.2006 N 149-ФЗ // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru дата обращения: 15.03.2022).
[14]Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности. Санкт-Петербург: СПбНИУИТМО, 2014. С 13.
[15]О безопасности : федеральный закон от 28.12.2010 N 390-ФЗ // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 15.02.2022).
[16]О персональных данных федеральный закон от 27.07.2006 N 152-ФЗ // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 15.02.2022).

Российской Федерации на рассмотрении находится Законопроект № 101234-8 «О внесении изменений в Федеральный закон "О персональных данных" и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных»[17], вносящий существенные изменения в процедуры, касающиеся трансграничной передачи данных и получения доступа персональных данных лиц, зарегистрированных в ЕГРЮЛ. Кроме того, предлагается внести новые обязать операторов уведомлять уполномоченные органы государственной власти об инцидентах, с принадлежащими таким операторам базами персональных данных.

В целях обеспечения безопасности сведений, представляющей государственную тайну, в РФ с 1993 года действует Федеральный Закон «О государственной тайне»[18]. Данным законом определяются сведения, являющиеся государственной тайной, а также установлен порядок засекречивания или рассекречивания информации. Помимо этого, закрепляется круг лиц, обладающих правом доступа к государственной тайне. Перечень лиц был предметом разбирательств в Конституционном Суде РФ, который в своих постановлениях отмечал, что секретность сведений сама по себе не может служить препятствием для ознакомления с материалами дела для участников, не обладающих доступом к государственной тайне[19].

Информация, представляющая собой коммерческую тайну, подлежит защите в РФ согласно Федеральному Закону «О коммерческой тайне»[20]. Данный закон определяет сведения, составляющие коммерческую тайну и регулируется порядок предоставления и охраны таких сведений.

---

[17]Законопроект N 101234-8 «О внесении изменений в Федеральный закон "О персональных данных" и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных» пространстве // Официальный интернет-портал правовой информации http://www.pravo.gov.ru (дата обращения:: 20.04.2022).

[18]О государственной тайне : закон Российской Федерации от 21.07.1993 N 5485-1 // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 01.01.2022).

[19] Постановление Конституционного Суда РФ : от 23.11.2017 по делу по делу о проверке конституционности статей 21 и 211 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина Е.Ю.Горовенко // Судебные и нормативные акты РФ – URL: http://www.sudact.ru (дата обращения: 01.01.2022).

[20]О коммерческой тайне : федеральный закон от 29.07.2004 N 98-ФЗ // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 01.01.2022).

На уровне подзаконных актов необходимо обратить внимание на многочисленные Указы Президента РФ. Такой вид подзаконных актов в первую очередь на утверждение стратегических документов РФ. Так Указом Президента Российской Федерации от 12 апреля 2021 года «Основы государственной политики Российской Федерации в области международной информационной безопасности»[21] закрепляется перечень основных угроз, цели и задачи государственной политики в информационной сфере, а также механизмы ее реализации на практическом уровне.

Сегодня, в условиях информационного противостояния указами также закрепляются меры, направленные на своевременную реакцию новым условиям информационной среды. Ярким примером может послужить Указ Президента РФ от 01.05.2022 N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»[22].

Важным является приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», ст. 2 которого устанавливает требования к «обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней при обработке указанной информации в государственных информационных системах»»[23].

Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в

[21]Основы государственной политики Российской Федерации в области международной информационной безопасности (утв. Указом Президента от 12.04.2021 N 213) // КонсультантПлюс : Справочная правовая система.—URL: http://www.consultant.ru/ (дата обращения: 15.02.2022).

[22]О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : указ Президента РФ от 01.05.2022 N 250 // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 10.05.2022).

[23]Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11.02.2013 N 17 // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 01.01.2022).

информационных системах персональных данных»[24] устанавливается регулирование в вопросах классификация информационных систем, направленных на обработку персональных данных граждан, а также закреплен перечень угроз и определены типы защищенности персональных данных.

Для комплексного анализа правового регулирования информационной безопасности необходимо к зарубежному законодательству. Научный интерес представляют такие страны как Германия и США, занимающие передовые позиции в области развития информационных технологий.

Отличительной чертой немецкого подхода к обеспечению информационной безопасности является его комплексный и фундаментальный характер, который включает разностороннюю систему нормативных актов, стратегических планов и институтов как на федеральном, так и на региональном уровнях.

Основными законодательными актами на федеральном уровне являются ФЗ «О вещательной деятельности», регулирующий правовую базу телемедиа в Германии, ФЗ «Об охране персональных данных», определяющий процедуры взаимодействия с такими данными, ФЗ «О порядке доступа к информации Федерального правительства", закрепляющий право каждого на получение официальной информации от государственных органов и ФЗ «О телекоммуникациях», направленный на поощрение конкуренции в области телекоммуникаций и эффективных телекоммуникационных инфраструктур.

В мае 2021 года был принят закон «О повышении безопасности информационных систем»[25], благодаря которому Федеральное агентство по кибербезопасности (das Bundesamt für Sicherheit in der Informationstechnik - BSI) получило новые полномочия, значительно укрепляющие его работу в качестве федерального агентства по кибербезопасности, например, BSI может

[24]Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ от 01.11.2012 N 1119 // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru (дата обращения: 11.01.2022).

[25]Zweites Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme// Bundesministerium der Justiz. Bundesamt für Justiz. Offizielle Webseite. – 2009. – URL: https://www.gesetze-im-internet.de/bsig_2009/ (дата обращения: 24.04.2022).

формировать программы по безопасной цифровизации и определять обязательные минимальные стандарты для федеральных властей и эффективно контролировать их соблюдение.

Такой стратегический документ ФРГ как белая книга 2016 года (Weißbuch)[26] закрепляет, что создание механизмов быстрого реагирования в ответ на нарастающие угрозы в информационном пространстве является одним из приоритетных направлений развития стратегии национальной безопасности Германии на ближайшее будущее.

В.В. Филатов в качестве особенности системы информационной безопасности США подчеркивает «тесное сотрудничество субъектов национальной безопасности и институтов гражданского общества в вопросах защиты интересов государства и граждан в информационной сфере»[27]. Вопросы информационной безопасности отражены в ряде специальных актов США. Так ФЗ «О свободе информации» закрепляет нормы, позволяющие полностью или частично обнародовать государственные документы США. Данный закон позволяет любому гражданину США делать запрос в федеральные органы США на получение все необходимой ему информации. Исключение составляют сведения, специально определенные законом (сведения о национальной обороне, личные документы граждан и т.д.). ФЗ «Об управлении информационной безопасностью» обязывает каждый государственный орган США разработать специальную программу, направленную на повышение информационной безопасности. ФЗ «О модернизации информационной безопасности», принятый в качестве ответа на возрастающее количество информационных атак на США, расширяет полномочия Правительства для оперативного реагирования на инциденты в информационной сфере.

В Стратегических документах США, такие как «Национальная стратегия кибербезопасности США», «Стратегия национальной безопасности США 2018», «Национальная стратегия физической защиты объектов

[26]Weißbuch 2016 Deutschland // Bundesministerium der Verteidigung. Offizielle Webseite. – 2016. – URL: https://www.bmvg.de/de/themen/dossiers/weissbuch (дата обращения: 21.03.2022).
[27]Филатов В.В. Зарубежный опыт правового регулирования информационной безопасности. 2018. С. 71.

жизнеобеспечения США» и «Временное руководство США по национальной безопасности» 2021 обращается внимание на стремительное развитие информационных технологий, что порождает возникновения новых потенциальных информационных угроз, для успешной борьбы с которыми США намерены активно развивать не только свою систему информационной безопасности, но и активно сотрудничать по данному вопросу с другими странами.

Основополагающую роль в правовой регламентации информационной безопасности играют принятые на международном уровне акты универсального, регионального и локального характера.

Одним из первых документов универсального характера, направленных на регулирования информационной безопасности, является Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[28], в которой выражается озабоченность возможного использования информационных технологий в неправовых целях, а также обозначен призыв к рассмотрению вопросов международного регулирования информационной безопасности и ее обеспечения.

В 2000 году по итогу Саммита G8 была принята Окинавская хартия[29], закрепляющая основные положения, на которые страны будут ориентироваться во время формирования и развития своей политики, а также приоритетные направления сотрудничества. По своей сущности данный документ является призывом к сокращению разрыва между странами в области информационных технологий.

В 2004 г. Российская Федерация подготовила документ под названием «Проект принципов, касающихся международной информационной

[28]Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Организация Объединенных Наций : Официальный сайт. – 1999. – URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения:: 12.04.2022).

[29]Окинавская хартия глобального информационного общества от 22.07.2000 // КонсультантПлюс : Справочная правовая система.—URL: http://www.consultant.ru/ (дата обращения: 11.01.2022).

безопасности». МИД РФ прокомментировал, что «данный документ содержит в себе основную понятийную базу и приводит ключевые определения международной информационной безопасности, угроз информационной безопасности, понятие информационного оружия, информационных войн, терроризма и информационной преступности»[30]. Пять принципов в области обеспечения международной информационной безопасности, закрепленные в данном проекте, были в итоге отражены в документе Генеральной Ассамблеи ООН A/55/140.

В 2016 – 2017 года была предпринята попытка утверждения документа под названием «Правила ответственного поведения государств в информационном пространстве в контексте международной безопасности»[31], однако по данному вопросу не был найден консенсус и в конечном итоге такие правила не были реализованы.

В 2018 году Генеральной Ассамблеей ООН была принята Резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[32], подчеркивающая необходимость выполнения международных обязательств в сфере информационно-коммуникационных технологий и Резолюция от 22 декабря 2018 г. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности»[33], подчеркивающая важность межгосударственного сотрудничества и следования ранее заключенным договоренностям.

[30]Mezhdunarodnoye sotrudnichestvo v oblasti informatsionnoj bezopasnosti [International cooperation in information security] // Министерство Иностранных Дел Российской Федерации. Официальный сайт. URL: http://www.mid.ru- /mezdunarodnaa-informacionnaa-bezopasnost/-/asset_-publisher/UsCUTiw2pO53/content/id/486848 (дата обращения: 10.04.2022).

[31]Правила ответственного поведения государств в информационном пространстве в контексте международной безопасности // Министерство Иностранных Дел Российской Федерации. Официальный сайт. URL: http://www.mid.ru- / (дата обращения: 11.04.2022).

[32]Резолюции A/RES/73/27 от 5 декабря 2018 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Организация Объединенных Наций. Официальный сайт. – 2018. – URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/ RES/53/70&referer=/english/&Lang=R (дата обращения: 10.04.2022).

[33]Резолюция A/RES/73/264 от 22 декабря 2018 г. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» // Организация Объединенных Наций. Официальный сайт. – 2018. – URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/ RES/53/70&referer=/english/&Lang=R (дата обращения: 10.04.2022)

Отличительной чертой большинства международных документов универсального характера является их рекомендательный характер, ввиду отсутствия юридической силы. Это позволяет квалифицировать их в качестве норм международного «мягкого права» (soft law). Такой подход объясняется большим количеством правовых проблем и нюансов, возникающих при попытках урегулирования отношений в области информационной безопасности. Именно поэтому в настоящее время отсутствует принятая на уровне ООН конвенция, касающаяся вопросов информационной безопасности, однако работа в данном направление активно ведется. Например, на сайте Совета Безопасности РФ можно ознакомиться с проектом концепции Конвенции ООН «Об обеспечении международной информационной безопасности»[34], которая содержит основные угрозы в области международной информационной безопасности, принципы, меры предотвращения конфликтов в информационном пространстве и т.д.

Международные акты регионального характера, напротив, как правило носят обязательный характер. Это обусловлено тем, что в разработке и принятии таких документов принимают участие страны, обладающие схожими взглядами и интересами. Примером могут служить акты Европейского Союза (ЕС).

Важную роль играет принятая 6 июля 2016 года Директива Европейского Парламента и Совета ЕС «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза»[35], впервые закрепляющая нормы регулирования информационной безопасности, обязательных для всех стран ЕС. Данная директива обязывает компаний, задействованных в важнейших секторах государственной деятельности (здравоохранение, банковская деятельность, энергетика и транспорт) сообщать

[34]Концепция Конвенции ООН «Об обеспечении международной информационной безопасности» // Совет Безопасности Российской Федерации. Официальный сайт. – 2011. – URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения: 12.04.2022).

[35]Директива Европейского Парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г. «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» // Справочная правовая система «КонсультантПлюс». — URL: http://www.consultant.ru / (дата обращения: 01.03.2022).

своим национальным властям о произошедших инцидентах, которые могут оказать влияние на систему информационной безопасности всего ЕС.

В целях достижения единообразия правового регулирования в области персональных данных, была принята Директива 2016/680 «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, ведения розыскных или судебных действий или исполнения уголовных наказаний, а также за свободное перемещение таких данных»[36] (GDPR), регулирующая процедуры получения, хранения, передачи и уничтожения персональных данных, а также механизмы соответствующего контроля.

Единственным европейским многосторонним актом, регулирующим вопросы противодействия преступности в информационной среде, является «Конвенция о преступности в сфере компьютерной информации»[37] 2001 года. Конвенция закрепляет перечень конкретных преступлений, связанных с использованием компьютерных технологий, а также формулирует рекомендации органам государственной власти по борьбе с такими преступлениями.

Стратегическими документами стран ЕС в области обеспечения информационной безопасности являются принятая в 2020 году стратегия кибербезопасности ЕС на цифровое десятилетие (The EU's Cybersecurity Strategy for the Digital Decade)[38], в рамках которой были определены такие стратегические инициативы как создание положения об информационной безопасности в институтах, органах и агентствах ЕС. В дополнение к данной стратегии было принято и положения об общих правилах кибербезопасности для институтов, органов и агентств ЕС. Стратегией подчеркивается

[36]Директива 2016/680 «О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, ведения розыскных или судебных действий, или исполнения уголовных наказаний, а также за свободное перемещение таких данных» // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 01.04.2022).

[37]Конвенция о преступности в сфере компьютерной информации ETS N 185 // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения 10.05.2022).

[38]The EU's Cybersecurity Strategy for the Digital Decade // European Commission. Official website. – 2020. – URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade (дата обращения: 12.05.2022).

необходимость дальнейшего сотрудничества между странами ЕС, ввиду нарастающего количества информационных угроз.

Таким образом, нормативно – правовая регламентация обеспечения информационной безопасности представляет собой многоуровневую систему нормативно - правовых актов, стратегий, концепций и резолюций, содержащих, как доктринальные положения, так и конкретные нормативно-правовые нормы, регулирующие различные аспекты информационной безопасности и обеспечивающих ее норм. Открытым остается вопрос большого количество норм «мягкого права» универсального характера. С одной стороны, необходимо учитывать интересы и государственный суверенитет, с другой стороны, ввиду рекомендательного характера таких норм, отсутствуют практические механизмы контроля и привлечения виновных к ответственности.

1.2. Понятие «информационная безопасность»

Понятие «информационная безопасность» в российском законодательстве является одним из базовых в области информационного права и национальной безопасности. Необходимо отметить, что данное понятие многоаспектно.

Генеральное определение, закрепленное в Доктрине информационной безопасности Российской Федерации от 2016 г. и продублированное в Стратегии национальной безопасности Российской Федерации, раскрывается как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[39]. Закрепленное содержание определяет первостепенные направления государства в области регулирования информационной безопасности.

[39]Доктрина информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 N 646) // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 15.02.2022).

Понятие «информационная безопасность» исследуют различные ученые еще с конца 90- ых - начала 2000-ых годов. М.В. Арсеньев определяет информационную безопасность как «снятие информационной неопределенности относительно объективно и субъективно существующих реальных и потенциальных угроз за счет контроля над мировым информационным пространством и наличие возможностей, условий и средств для отражения этих угроз, что в совокупности определяют степень информационной безопасности субъекта информационного права» [40]. Похожая точка зрения наблюдается у Д.А. Ловцова, который рассматривает информационную безопасность как «определенное свойство для объекта либо субъекта информационного права, которое определяет уровень защищенности в качественной информации для дальнейшего функционирования и развития»[41].

В противоположность вышеназванным мнениям, А.Д. Урсул определяет информационную безопасность как «состояние защищенности в информационной среде по отношению к внутренним и внешним угрозам»[42].

В.Н. Лопатин также определяет исследуемое понятие как «состояние защищенности, интересов как личности и общества, так и государства от воздействия вредной информации».[43]

А.А. Стрельцов указывает, что «данный институт был определен как явление, которое формируется за счет различных потребностей государства в информационной среде».[44]

Т.В. Закупень, изучая понятие информационной безопасности, отмечает не только чисто технической характер и считает, что данное понятие «скорее социальное, нежели чисто техническое явление. Ее нельзя отождествлять с применением специальных технических средств и методов для защиты

[40]Арсентьев М.В. К вопросу о понятии «информационная безопасность».1997. С. 51.
[41]Ловцов Д.А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере. 2015. № 2. С. 53.
[42]Урсул А.Д. Информационная стратегия и безопасность в условиях устойчивого развития. 1996. С. 6.
[43]Лопатин В.Н. Информационное право: Учебник. СПб: Юридический центр Пресс, 2005.С 409.
[44]Стрельцов А.А. Содержание понятия «обеспечение информационной безопасности».2001. С. 11.

информации от несанкционированного доступа, похищения, уничтожения и т.д.»[45] .

С.В. Иванов под информационной безопасностью понимает «состояние высокой степени защищенности личности при котором гарантируется реализация ее прав и свобод в информационной сфере и максимально снижен риск негативного воздействия на нее внутренних и внешних угроз».[46]

Наиболее точно и полно данное определение было раскрыто профессором Т.А. Поляковой, которая определяет информационную безопасность как «состояние защищенности национальных интересов Российской Федерации в информационной сфере, состоящих из совокупности сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз, что соответствует принципу обеспечения национальной безопасности в информационной сфере, определенному в Стратегии развития информационного общества в Российской Федерации»[47].

А.В. Зенков придерживается схожей точки зрения и раскрывает анализируемое понятие как «защищенность информации от незаконного получения, преобразования и уничтожения, а также защищённость информационных ресурсов от воздействий, направленных на нарушение их работоспособности» [48]. Аналогичного определения придерживается и В.Ф. Шаньгина[49].

В.Н. Ясенева, А.В Дорожкина и А.Л Сочкова выводят на первый план свойство защиты, раскрывая информационную безопасность как «невозможность причинения вреда свойствам объекта безопасности, которые обусловлены информацией и информационной инфраструктурой».[50]

---

[45]Закупень Т.В. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ. 2009. С. 31.

[46]Иванов С.В. Правовое регулирование информационной безопасности личности в Российской Федерации. Вестник Екатерининского института.2014. С. 50.

[47]Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России. Автореф. дис. …докт. юрид. наук: 12.00.14. Москва, 2008. С. 18.

[48]Зенков А.В. Информационная безопасность и защита информации: учебное пособие для вузов. 2021. С. 53.

[49]Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. 2011. С. 265.

[50]Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Информационная безопасность: учеб. Пособие, под общ. ред. В.Н. Ясенева. 2017. С 9.

Х.В. Идрисов под информационной безопасностью понимает «такое состояние информационных источников, предполагающее их эффективную защиту от воздействия угроз при получении, обработке, хранении и передаче информации, посредством обеспечения доступности, целостности и конфиденциальности информации при реализации акторами мер защиты информации частного, государственного и межгосударственного характера»[51].

Таким образом, большинство авторов, отмечают, что информационная безопасность это прежде всего состояние защищенности, обеспечивающие безопасность информации и информационных источников и отвечающая интересам личности, общества и государства. Такого подхода отражен в Доктрине информационной безопасности 2016г.

Отметим, что закон Российской Федерации «О безопасности критической информационной структуры в РФ» [52] закрепляет понятие «безопасность критической информационной инфраструктуры». Данное понятие является более узким, по отношению к понятию «информационная безопасность», так как относится к специальному объекту защиты – критическая информационная инфраструктура Российской Федерации, под которой понимается «информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления»[53].

Для более точного нормативного определения информационной безопасности необходимо рассмотреть иностранные законодательства и междунродно – правовые акты.

Приложение 1 к межправительственному Соглашению между членами Шанхайской Организации «О сотрудничестве в области обеспечения международной информационной безопасности»[54] закрепляет исследуемое

[51]Идрисов Х.В. Информационная безопасность как один из элементов национальной безопасности. 2021. С. 157.
[52]О безопасности критической информационной инфраструктуры Российской Федерации : федеральный закон от 26.07.2017 N 187-ФЗ // КонсультантПлюс : Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 14.04.2022).
[53]Там же.
[54]Межправительственное соглашение между членами Шанхайской Организации о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // Шанхайская организация сотрудничества. Официальный сайт. URL: http://rus.sectsco.org (дата обращения: 21.04.2022).

понятие как «состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве».[55] Соглашение «О сотрудничестве государств - членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности»[56] содержит схожий вариант понятия информационной безопасности. Такой подход к раскрытию содержания понятия «информационная безопасность» аналогичен подходу в законодательстве Российской Федерации.

Иные подходы к определению информационной безопасности можно наблюдать в зарубежных странах. В 2001 году в сообщении Европейской Комиссии под названием «Сетевая и информационная безопасность: предложения для подхода европейской политики»[57] был закреплено понятие «Сетевая и информационная безопасность» (Network and Information Security), под которым понималась «способность сети или информационной системы противостоять при заданном уровне надежности случайным событиям или вредоносным действиям. Такие события или действия могут поставить под угрозу доступность, подлинность, целостность и конфиденциальность хранимых или передаваемых данных, а также связанных с ними услуг, предлагаемых через эти сети и системы»[58].

Позднее Директива Европейского Парламента и Совета ЕС 2016/1148 от 6 июля 2016 г. закрепила понятие «Сетевая и информационная безопасность», которая определяется как «способность сетевых и информационных систем на заданном уровне надежности противостоять любым действиям, угрожающим доступности, достоверности, целостности или конфиденциальности хранимых, передаваемых или обрабатываемых данных или связанных с ними услуг,

[55] Там же.
[56]Соглашение «О сотрудничестве государств - членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности» [Электронный ресурс] // Организация договора о коллективной безопасности. Официальный сайт. URL: https://odkb-csto.org/ (дата обращения: 20.04.2022).
[57]Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach /* COM/2001/0298 final * // European Union. Official website. – 2010. – URL: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:52005DC0389 (дата обращения: 20.04.2022).
[58]Там же.

предлагаемых или доступных через указанные сетевые и информационные системы»[59].

Законодательство ФРГ в Законе «О телекоммуникациях»[60], закрепляет аналогичное Директиве ЕС 2016/1148 от 6 июля 2016 года понятие «Безопасность сетей и сервисов».

Кроме того, закон «О Федеральном управлении информационной безопасности Германии» (BSIG) содержит такое понятие как «Безопасность информационных технологий», под которым подразумевается «соблюдение определенных стандартов безопасности, касающихся доступности, целостности или конфиденциальности информации, с помощью мер безопасности в информационно-технических системах, компонентах или процессах, а также при применении информационно-технических систем»[61].

В США понятие «информационная безопасность» закреплено в законе «Об управлении информационной безопасностью» от 2002 года (Federal Information Security Management Act of 2002) и рассматривается как «защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, изменения или уничтожения в целях обеспечения целостности, конфиденциальности и доступности»[62]. Стратегические документы США, такие как Стратегия национальной кибербезопасности 2018 года, Стратегия национальной безопасности 2018 года и Временное руководства США по национальной безопасности 2021 года содержат лишь указания на то, что информационная безопасность и ее обеспечение является одним из приоритетных стратегических направлений развития США.

---

[59]Директива Европейского Парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г. «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» // КонсультантПлюс : Справочная правовая система.—URL: http://www.consultant.ru/ (дата обращения: 01.01.2022).

[60]Telekommunikationsgesetz // Bundesministerium der Justiz. Bundesamt für Justiz. Offizielle Webseite. – 2021. – URL: https://www.gesetze-im-internet.de/tkg_2021/BJNR185810021.html (дата обращения: 21.02.2022).

[61]Gesetz über das Bundesamt für Sicherheit in der Informationstechnik // Bundesministerium der Justiz. Bundesamt für Justiz. Offizielle Webseite. – 2009. – URL: https://www.gesetze-im-internet.de/bsig_2009/ (дата обращения: 24.04.2022).

[62]Federal Information Security Management Act of 2002 [Электронный ресурс] // the federal government of the United States. Library of Congress. Official website. – 2002. – URL: https://www.congress.gov/ (дата обращения: 20.04.2022).

На практике информационная безопасность в рамках управления ИТ-безопасностью, опирается на международную серию ISO/IEC-27000, например, международным стандартом ISO/IEC 27000:2018 информационная безопасность рассматривается как «сохранение конфиденциальности, целостности и доступности информации. Кроме того такой стандарт подчеркивает и другие свойства как подлинность, подотчетность, неотказуемость (non-repudiation) и надежность»[63]. Под неотказуемостью понимается «способность доказать возникновение заявленного события или действия и его исходных объектов»[64].

Национальным институтом стандартов и технологий США (National Institute of Standards and Technology) исследуемое понятие раскрывается как «защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, изменения или уничтожения в целях обеспечения конфиденциальности, целостности и доступности»[65].

Н.П. Ромашника и В.Г. Задремайлова при анализе китайского подхода к регулированию вопросов информационной безопасности отмечают, что в КНР информационная безопасность рассматривается как «защита оборудования, программного обеспечения, данных и предоставляемых услуг информационной системы, с исключением вероятности несанкционированного доступа к ним, утечки, уничтожения или изменения по случайным или злонамеренным причинам, просмотра, проверки, записи или уничтожения, с целью обеспечения непрерывной и надежной работы информационной системы»[66]. Кроме того, в обзоре актов, связанных с регулированием вопросов информационной безопасности Китая отмечено, что исполнение требований конфиденциальности, подлинности, целостности, безотказности, готовности,

[63]Information security standards ISO/IEC 27000:2018 // International Organization for Standardization. Official website. – 2018. – URL: https://www.iso.org/ru/standard/73906.html (дата обращения: 13.03.2022).
[64]Там же.
[65]Glossary of National Institute of Standards and Technology // National Institute of Standards and Technology. Official website. – 2022. – URL: https://csrc.nist.gov/glossary/term/information_security (дата обращения: 13.03.2022).
[66]Ромашкина Н.П., Задремайлова В.Г. Эволюция политики КНР в области информационной безопасности // Пути к миру и безопасности. 2020. С. 123.

проверяемости и управляемости является основным элементом информационной безопасности.

Национальным информационным консультативным комитетом КНР информационная безопасности определяется как «ключевой компонент системы национальной безопасности, который необходим для обеспечения устойчивого, здорового применения информационных технологий, а также для социальной и культурной стабильности и идеологического развития»[67].

Таким образом, зарубежное законодательство раскрывает содержание понятия «информационная безопасность», указывая на необходимость соблюдения конфиденциальности, целостности и доступности. Следовательно, для более полного определения информационной безопасности, необходимо раскрыть данные понятия.

Доступность – это возможность субъекта получить необходимую информационную услугу в определённый промежуток времени. В США, например, под доступностью понимается «обеспечение своевременного и надежного доступа к информации и ее использованию»[68].

Федеральный закон «Об управлении информационной безопасностью» США определяет конфиденциальность как «сохранение разрешенных ограничений на доступ и раскрытие информации, включая средства защиты личной конфиденциальности и конфиденциальной информации»[69].

Целостность раскрывается как актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения. В.В. Гафнер, считает, что «целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий

[67]2006-2020 年国家信息化发展战略 (2006-2020 Nián guójiā xìnxī huà fāzhǎn zhànlüè; The State strategy for the development of informatization for the period from 2006 to 2020) // China government. Official website. – 2006. – URL: https://baike.baidu.com/item /2006-2020%20%E5%B9%B4%E5%9B%BD%E5%AE%B6%E4%BF%A1%E6%81%AF%E5%8C%96%E5% 8F%91%E5%B1%95%E6%88%98%E7%95%A5 (дата обращения: 13.04.2022).

[68]Federal Information Security Management Act of 2002 // the federal government of the United States. Library of Congress. Official website. – 2022. – URL: https://www.congress.gov/ (дата обращения: 23.03.2022).

[69]Federal Information Security Management Act of 2002 // the federal government of the United States. Library of Congress. Official website. – 2022. – URL: https://www.congress.gov/ (дата обращения: 23.03.2022).

(транзакций))»[70]. В США Закон «Об управлении информационной безопасностью» раскрывает данное понятие как «защиту от ненадлежащего изменения или уничтожения информации, включая обеспечение неразглашения и подлинности информации»[71].

Анализ зарубежного законодательства и международно – правовых источников показывает, что иностранные подходы к определению понятия информационной безопасности и раскрытию ее содержания во много имеет сходства с закрепленным в Федеральном Законе «Об информации, информационных технологиях и защите информации»[72]. Понятие «защита информации» также как и зарубежные акты предусматривает обеспечение защиты информации от несанкционированного доступа, при реализации требований доступности, целостности и конфиденциальности.

Однако информационная безопасность не ограничивается исключительно защитой информации. В.В. Гафнер придерживается мнения, что «меры по обеспечению информационной безопасности должны осуществляться в разных сферах – политике, экономике, обороне, а также на различных уровнях – государственном, региональном, организационном и личностном. Поэтому задачи информационной безопасности на уровне государства отличаются от задач, стоящих перед информационной безопасностью на уровне организации»[73]. Следовательно, такой подход не соответствует многоаспектному подходу к определению информационной безопасности.

Еще одним проблемным вопросом является разграничение понятий «информационная безопасность» и «кибербезопасность».

Кибербезопасность в узком смысле понимается как практика защиты критически важных систем и конфиденциальной информации от цифровых атак. Схожие определения закрепляют Центр обмена и анализа информации

[70]Гафнер В.В. Информационная безопасность: учебное пособие в 2 ч. Ч.1. 2009. С. 21.
[71]Federal Information Security Management Act of 2002 [Электронный ресурс] // the federal government of the United States. Library of Congress. Official website. URL: https://www.congress.gov/ (дата обращения: 16.03.2022).
[72]Об информации, информационных технологиях и о защите информации : федеральный закон от 27.07.2006 N 149-ФЗ (последняя редакция) // КонсультантПлюс : Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 01.01.2022).
[73]Гафнер В.В. Информационная безопасность: учебное пособие в 2 ч. Ч.1. 2009. С. 19.

(Information Sharing and Analysis Center - ISAC) и Международная организация по стандартизации (International Organization for Standardization – ISO). Однако такое узкое толкование понятия «кибербезопасность» не позволяет провести разграничение с информационной безопасностью.

В более широком смысле, кибербезопасность раскрывается как «Кибербезопасность – это область информационных технологий, ориентированная на защиту систем, включающих в себя электронные записи, устройства для отслеживания информации, оборудование и программное обеспечение, используемое для оказания услуг и управления ими. Кибербезопасность направлена на предотвращение атак путем защиты систем от несанкционированного доступа, использования и раскрытия данных»[74]. Основным направление кибербезопасности является предотвращение атак путем обеспечения защиты систем от несанкционированного доступа, раскрытия и использования данных. Основная цель кибербезопасности – это обеспечение доступности, конфиденциальность и целостности данных.

Если мы обратимся к определению понятия «информационная безопасность» от NSTI (см. выше), то заметим, что информационная безопасность преследует те же цели, что и кибербезопасность, однако информационная безопасность - это более широкая категория средств защиты, связанная с обеспечением безопасности информации, от угроз, не связанных с личностью, например, стихийные бедствия. Любые внешние носители (диски, дискеты, USB-флэш-накопители, внешние жестки диски и т.д.), документы, чертежи, фотографии - все эти элементы находятся в рамках информационной безопасности. Кибербезопасность в свою очередь обеспечивает защиту цифровой информации (сети, программы, устройства, серверы и др.).

Таким образом кибербезопасность – это информационная безопасность, но в цифровой сфере, в связи с чем к ней применяются такие же правила, что и к информационной безопасности.

[74]Козлова Н.Ш., Довгаль В.А. Кибербезопасность и информационная безопасность: сходства и отличия. 2021. С. 91.

Таким образом, проанализировав подходы к раскрытию понятия информационная безопасность в РФ и за рубежом можно сделать следующие выводы:

1) В РФ данное понятие закреплено только на стратегическом уровне, ввиду многоаспектного содержания данного понятия. Именно поэтому Законы РФ не содержат легального определения информационной безопасности. На законодательном уровне, в целях реализации Доктрины информационной безопасности РФ, были закреплены специальные определения - «Безопасность критической информационной инфраструктуры» и «Защита информации», играющие практическую роль в реализации технического аспекта информационной безопасности. Для реализации других аспектов принимаются соответствующие правовые акты, например, многочисленные указы Президента РФ, направленные на политический аспект обеспечения информационной безопасности. В иностранных государствах, таких как Германия, Китай и США наблюдается аналогичный подход. Как правило информационная безопасность является стратегическим направлением деятельности государства, а на законодательном уровне закрепляется целый ряд более узких понятий, совокупность которых и образует многоаспектное правовое регулирование информационной безопасности.

2) Российская Федерация, закрепляя информационную безопасность как «состояние защищенности», не раскрывает содержание данной защищенности. Невозможно определение защищенности через цели, указанные в Доктрине информационной безопасности 2016, так как их расплывчатое закрепление позволяет осуществлять широкое толкование.

Системное толкование позволяет раскрыть содержания защищенности через защиту информации. Определённые Федеральным Законом «Об информации, информационных технологиях и защите информации»[75] цели, позволяют раскрыть защищенность как состояние, гарантирующее

[75]Об информации, информационных технологиях и о защите информации : федеральный закон от 27.07.2006 N 149-ФЗ // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 25.01.2022).

конфиденциальность, доступность и целостность информации и информационных систем. Аналогичный подход используется иностранными законодательствами при толковании определений защиты информации, информационных систем и информационной безопасности в целом.

Однако российский вариант информационной безопасности представляет собой более широкий подход и охватывает не только защищенность информации и информационных систем, но важность соблюдения интересов личности, общества и государства, что подчёркивает невозможность определения состояния защищенности только на основе технических требований, предъявляемых к защите информации и информационных систем. В связи с этим необходима разработка более четких критериев защищенности, отвечающих, как технической составляющей информационной безопасности, так и социальной.

1.3. Принципы информационной безопасности

Вся государственная деятельность основывается на определенных принципах и деятельность по обеспечению информационной безопасности не является исключением. С учетом многоаспектности изучаемого вопроса все принципы подразделяются на две большие группы – государственные и международные.

Государственные принципы направлены на регулирования организации деятельности информационной безопасности в отдельно взятой стране и как правило служат основой для правового аспекта информационной безопасности.

Для определения государственных принципов обеспечения информационной безопасности в РФ необходимо обратиться к Федеральному закону «О безопасности», ст. 2 которого закрепляются такие принципы обеспечения безопасности Российской Федерации как:

1. «Соблюдение и защита прав и свобод человека и гражданина;
2. Законность;

3. Системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;
4. Приоритет предупредительных мер в целях обеспечения безопасности;
5. Взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности»[76];

Под принципом законности в широком смысле понимается исполнение и соблюдение всеми органами государственной власти, физическими и юридическими лицами требований действующего законодательства РФ, в том числе имплементированных норм международного права. Законность является ядром правового государства и одним из базовых элементов правового и демократического развития общества. В.А. Мазуров и В.А. Невинский приходят к выводу, что данный принцип «служит базой для законотворчества в части обеспечения защиты информации, информационной структуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, системы регулирования возникающих при этом отношений, требует, чтобы содержание всех законов соответствовало положениям конституции РФ, международным договорам и соглашениям России с зарубежными государствами, заключенными для координации и взаимодействия в вопросах противодействия преступным посягательствам в информационной сфере»[77]. Все, кто задействован в обеспечении

[76]О безопасности : федеральный закон от 28.12.2010 N 390-ФЗ // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 16.02.2022).
[77]Мазуров В.А., Невинский В.В. Понятие и принципы информационной безопасности. 2003. С. 62.

информационной безопасности обязаны соблюдать требования действующего российского законодательства.

Вызывает вопрос закрепление соблюдения и защиты прав и свобод человека и гражданина в качестве самостоятельного принципа. Статься 2 Конституции РФ гласит: «Соблюдение и защита прав и свобод человека и гражданина является конституционной обязанностью государства»[78]. Статьей 45 Конституции РФ гарантируется государственная защита прав и свобод человека и гражданина[79]. Соблюдение действующих положений законодательства, в том числе и Конституции, является воплощения принципа законности. Таким образом, соблюдение и защита прав и свобод человека и гражданина охватывается принципом законности.

Второй принцип закрепляет применение мер различного характера, необходимых для обеспечения информационной безопасности. Как было отмечено выше, информационная безопасность состоит не только из технических и цифровых аспектов, но и включает в себя правовые, социально - экономические, политические и организационные элементы. Все они находятся в плотной взаимосвязи между собой, выстраивая тем самым четкую системы правоотношений между субъектами, задействованных в области информационной безопасности и ее обеспечения. Следовательно, для успешного функционирования такой разнообразной системы общественных отношений необходимо применение различных мер, отвечающих особенностям определенного элемента системы, например, для политического элемента характерно принятие конкретных политических решений, правовые меры необходимы для регулирования деятельности и процедур и т.д.

Принцип, закрепляющий приоритет предупредительных мер в целях обеспечения безопасности закрепляют одну из важнейших задач информационной безопасности – своевременное обнаружение признаков угроз

[78]Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 01.01.2022).
[79]Там же.

и их анализ. Именно адекватные превентивные меры позволяют избегать возникновения угроз в области информационной безопасности, понижая тем самым вероятность неправомерных действий в данной сфере.

Последний принцип, закрепленный ФЗ «О безопасности», подчеркивает важность взаимодействия государства с международными организациями и гражданским обществом. Данный принцип позволяет обмениваться знаниями и опытом с гражданским обществом, а также получать ответную реакцию на проводимую государством политику в области информационной безопасности. Такое взаимодействие необходимо для полноценного и многостороннего развития системы информационной безопасности.

В.А. Мазуров и В.А. Невинский предлагают выделить принцип обоснованности. Согласно данному принципу, защите подлежит только та информация, которая наносит существенный вред охраняемым законом интересам в случае ее незаконного использования, получения и (или) распространения. В связи с этим, по мнению указанных авторов «принцип обоснованности заключается в установлении путем экспертной оценки целесообразности ограничения доступа к конкретной информации, выделении вероятных экономических и иных последствий этого акта исходя их баланса жизненно важных интересов личности, общества, государства, разработки адекватных мер противодействия внешним и внутренним угрозам информационной безопасности»[80].

Выделение принципа обоснованности в том варианте, в котором он описан выше, распространяется только на защиту информации, а информационная безопасность подразумевает «состояние защищенности личности, общества и государства». Обеспечение информационной безопасности, нацеленное на создание такого состояния, подразумевает не только защиту информации, но и другие виды деятельности. Таким образом принцип обоснованности распространяется не на все меры, необходимые для

[80]Мазуров В.А., Невинский В.В. Понятие и принципы информационной безопасности. 2003. С. 62.

обеспечения информационной безопасности, что не вызывает необходимости для выделения обоснованности в качестве отдельного принципа.

Что касается принципов, закрепленных в зарубежных законодательствах, то, например, США в своих стратегических документах ссылаются на такие принципы как защита основных прав и свобод, защита права собственности, ценность частной жизни, защита от преступлений и право на самооборону. Помимо этого, подчеркивается важность укрепления принципов прозрачности деятельности правительства и свободного демократического общества. Такие принципы не являются специальными и лежат в основе любой государственной деятельности. Что касается специальных принципов, то они были закреплены национальной стратегии кибербезопасности США в которой отмечено стремление США «развивать принципы «открытого, функционально совместимого, интероперабельного, надежного и безопасного интернета»[81].

В ФРГ информационная безопасность в первую очередь базируется на конституционных принципах, а именно на принципах законности, федерализма и равенства. Анализ же стратегических документов ФРГ отсылает к общеевропейским принципам информационной безопасности, поэтому далее необходимо проанализировать европейские акты, закрепляющие принципы обеспечения информационной безопасности.

Так, например, Директива Европейского Парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г. «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза»[82] в своем тексте отсылает к принципам, закрепленным Хартией Европейского союза «Об основных правах»[83]. Данная Хартия закрепляет такие принципы правовых государств как законность, равенство, субсидиарность, устойчивое развитие,

[81]National cyber strategy of the United States of America 2018 // White House. Official website – 2018. – URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 13.04.2022).
[82]Директива Европейского Парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г. «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» // КонсультантПлюс: Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 01.01.2022).
[83]Хартия Европейского Союза об основных правах 2007/С 303/01 // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 01.05.2022).

взаимосвязь с гражданским обществом и другие. Все они также являются общими принципами и не были специально разработаны для регулирования деятельности в области информационной безопасности.

Международные принципы информационной безопасности, в отличие от государственных принципов, направлены на регулирование политического элемента информационной безопасности и сводятся к установлению основ межгосударственного взаимодействия.

Так, упомянутый ранее документ Генеральной Ассамблеи ООН A/55/140, созданный на основе проекта принципов международной информационной безопасности, подготовленного РФ, содержит пять основных принципов – право на участие всех субъектов международного права в информационном пространстве, ограничение угроз в сфере международной информационной безопасности, укрепление международного сотрудничества, мирное урегулирование споров и ответственность государств за нарушение названных принципов. Выделение таких принципов является основой для принятие будущих документов, необходимых для регулирования международной информационной безопасности.

Отметим также на предложенную Российской Федерацией концепцию Конвенции ООН «Об обеспечении международной информационной безопасности»[84], в которой закреплен целый ряд принципов, таких как суверенитет, равенство, свобода и самостоятельность, законность, неделимость безопасности и др. Данные принципы также могут послужить ориентирами как для существующего межгосударственного взаимодействия, так и основой для заключения межгосударственных соглашений.

Представляет интерес подход ОБСЕ к регулированию вопросов, связанных с информационной безопасностью. В настоящее время не принято единого документа, закрепляющего конкретные права и обязанности государств участниц ОБСЕ в области обеспечения информационной

[84]Концепция Конвенции ООН «Об обеспечении международной информационной безопасности» // Совет Безопасности Российской Федерации. Официальный сайт. – 2011. – URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения: 12.04.2022).

безопасности. Тем не менее, в Решении № 1202 «Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий»[85] был закреплен ряд общих принципов, которыми должны руководствоваться государства при взаимодействии в данной области. К таким принципам относятся добровольность, сотрудничество, обмен опытом, мирное урегулирование конфликтов. В данном документе подчеркивается важность обеспечения «открытости, функциональной совместимости, безопасности и надежности Интернета»[86].

Целый ряд международных принципов закреплен в документах региональных организаций. В ст. 4 Соглашения между членами Шанхайской Организации «О сотрудничестве в области обеспечения международной информационной безопасности» закреплена приверженность общепринятым принципам международного права, а также принципам невмешательства и регионального сотрудничества. Отмечается право каждый стороны данного соглашения на поиск, получение и распространение информации, а также право на защиту информационных ресурсов и критически важных структур от несанкционированного вмешательства.

Хотелось бы также отметить Модельный закон ОДКБ «Об информационной безопасности»[87], который является правовым ориентиром для стран участниц ОДКБ. В статье 2 данного закона закреплена важность сотрудничества стран участниц ОДКБ в области информационной безопасности. Документ подчеркивается равенство в обеспечении права на защиту своих информационных ресурсов и отмечается недопустимость враждебных действий в информационном пространстве по отношению к друг другу.

[85]Решение № 1202 «Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» // ОБСЕ. Официальный сайт. – 2016. – URL: https://www.osce.org/files/f/documents/e/4/228521.pdf (дата обращения: 13.03.2022).
[86]Там же.
[87]Модельный закон ОДКБ «Об информационной безопасности» [Электронный ресурс] // ОДКБ. Официальный сайт. URL: https://paodkb.org/ (дата обращения: 13.05.2022).

Таким образом, принципы обеспечения информационной безопасности разделяется на две большие группы – государственные и международные. Существование такого разделения обусловлено многоаспектностью информационной безопасности. Государственными принципами регламентируется деятельность, направленная на обеспечение информационной безопасности отдельно взятого государства в рамках его юрисдикции, в то время как международные принципы представляют собой базу для международного сотрудничества в рамках обеспечения информационной безопасности.

Глава 2. Обеспечение информационной безопасности

2.1. Угрозы информационной безопасности и их виды

Бурное развитие систем информационной безопасности неизбежно порождает развитие новых информационных угроз. По данным экспертов, ущерб, нанесенный в результате неправомерных действий в информационном пространстве может составить примерно 90 триллионов долларов к 2030 году. В связи с этим остро встает вопрос определения угроз информационной безопасности и разграничения их по определённым критериям, с целью выработки оптимальной стратегии противодействия таким угрозам.

В доктрине существуют различные подходы к определению угроз информационной безопасности. Так как информационная безопасность является элементом общественной безопасности, то имеет смысл обратить внимание на определение угрозы общественной безопасности, данное Н.А. Босхамжиевой, которая отмечает, что «угроза общественной безопасности представляет собой возможность причинения ущерба охраняемым законом правам и свободам личности, материальным и духовным ценностям общества, конституционного строя, суверенитета и территориальной целостности»[88]

Е.О. Напханенко, изучая угрозы информационной безопасности в контексте интернет пространства считает, что «угроза информационной безопасности в сети Интернет представляет собой совокупность факторов и их последствий, создающих реальную и потенциальную опасность состоянию защищенности национальных интересов государства, общества и личности в информационной сфере сети Интернет»[89].

В Российской Федерации в Стратегии Национальной безопасности закреплено общее понятие «угроза национальной безопасности», которое определяется как «совокупность условий и факторов, создающих прямую или

[88]Босхамджиева Н.А. Понятие угрозы общественной безопасности. 2012. С. 42.
[89]Напханенко Е.О. Понятие и классификация информационных угроз в сети Интернет. 2011. С. 125.

косвенную возможность причинения ущерба национальным интересам Российской Федерации»[90]

В разделе III Доктрины информационной безопасности Российской Федерации закреплены положения, направленные на регулирование информационной угрозы. Согласно данной доктрине угроза информационной безопасности (информационная угроза) представляет собой «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере»[91]. Так как в РФ одинаковое смысловое значение имеют понятия «угроза информационной безопасности» и «информационная угроза» в дальнейшем представляется возможным использование двух этих понятий в отношении изучаемого вопроса.

Доктрина 2016 года использует широкий подход к определению информационных угроз. Это происходит как констатированием общей проблемы использования информационного – технического потенциала в отношении важных инфраструктур государства, так и путем перечисления конкретных угроз, например, компьютерная преступность, использования информационных технологий террористическими и экстремистскими организациями, дестабилизация внутриполитической ситуации и т.д.

В зарубежном законодательстве перечислены информационные угрозы. Законодательство ФРГ не содержит конкретного понятия «информационная угроза». Тем не менее, в законе «О Федеральном управлении информационной безопасности Германии» (BSIG) закреплено понятие «вредоносные программы» под которыми понимается «программы и другие информационные процедуры, которые служат целям несанкционированного использования или удаления данных, или которые служат целям несанкционированного

[90]Доктрина национальной безопасности Российской Федерации : указ Президента РФ от 02.07.2021 N 400 // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 21.05.2022).
[91]Доктрина информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 N 646 // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 15.05.2022).

воздействия на другие информационные процессы»[92]. Кроме того, данный закон обращает внимание на такое понятие как «уязвимость», под которым подразумевается свойство программ или других информационных систем, использование которых может позволить третьим лицам получить доступ к чужим информационным системам против воли законного лица или повлиять на функционирование информационно-технических систем.

В США исполнительным указом «О совершенствовании национальной кибербезопасности» закрепляется понятие «инцидент», под которым подразумевается означает «событие, которое без законных полномочий, фактически или неизбежно ставит под угрозу, целостность, конфиденциальность, доступность информации или информационной системы либо представляет собой нарушение или непосредственную угрозу нарушения закона, политик безопасности, процедур безопасности или политик допустимого использования»[93].

Отметим разнообразные подходы к определению информационной угрозы на региональном уровне. Так Директива Европейского Парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г. «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» также содержит понятие «инцидент», под которым подразумевается «событие, оказывающее непосредственное отрицательное воздействие на сетевые и информационные системы»[94].

Межправительственное соглашение между членами Шанхайской Организации «О сотрудничестве в области обеспечения международной информационной безопасности» под угрозой информационной безопасности

[92]Gesetz über das Bundesamt für Sicherheit in der Informationstechnik [Электронный ресурс] // Bundesministerium der Justiz. Bundesamt für Justiz. Offizielle Webseite. URL: https://www.gesetze-im-internet.de/bsig_2009/ (дата обращения: 24.04.2022).

[93]Executive Order on Improving the Nation’s Cybersecurity 12 Mai 2021 // The White House. Official website. – 2021. – URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (дата обращения: 24.04.2022).

[94]Директива Европейского Парламента и Совета ЕС (ЕС) 2016/1148 от 6 июля 2016 г. «О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза» // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 22.04.2022).

понимает «факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве»[95].

Различные подходы отмечаются также и в классификации информационных угроз. Например, в основах государственной политики Российской Федерации в области обеспечения международной информационной безопасности, в пункте 8 закреплен перечень информационных угроз. К ним относятся:

«а) использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;

б) использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

в) использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;

г) использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;

д) использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;

е) использование отдельными государствами технологического доминирования в глобальном информационном пространстве для

[95]Межправительственное соглашение между членами Шанхайской Организации «О сотрудничестве в области обеспечения международной информационной безопасности» // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 22.04.2022).

монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства»[96].

Анализ вышеназванных угроз позволяет сделать вывод, что на стратегическом уровне Российской Федерацией используется широкий подход к закреплению понятия информационной угрозы и ее видов. Критерием для разграничения информационных угроз между собой выступает «цель использования информационных – коммуникационных технологиях».

Как было отмечено выше, информационная безопасность является стратегическим понятием, а на законодательном уровне регулируются более узкие, специальные ее элементы. Одним из таких элементов является защита информации, поэтому представляется важным квалифицировать информационные угроз в соответствии с критерием требований, предъявляемых к защите информации. Основываясь на данном критерии можно выделить следующие виды информационных угроз:

1. Нарушение конфиденциальности информации («Утечка»).Данная угроза представляет собой вероятность получения неправомерного доступа к защищаемой информации. Угроза возникает каждый раз, когда у неуполномоченного лица возникает неправомерная возможность воспользоваться охраняемой информацией.

2. Нарушения целостности информации. Под данной угрозой подразумевается возможность воздействия на целостность информации, путем ее нелегального изменения. Умышленное, неправомерное изменение информации нарушает ее целостность. Нарушение целостности также возможно, если несанкционированное изменение охраняемой информации было вызвано ошибками в системах программного или аппаратного

[96]Основы государственной политики РФ в области обеспечения международной информационной безопасности : указ Президента РФ от 12.04.2021 N 213 // КонсультантПлюс : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения: 10.04.2022).

обеспечения. При этом необходимо отметить, что правомерное изменение целостности информации не представляет собой информационной угрозы.

3. Такая угроза как нарушение доступности информации заключается в наличии возможности несанкционированной блокировки доступа к информации или к информационному ресурсу. Необходимо отметить, что такое блокирование может иметь постоянный характер, т.е. доступ к такому ресурсу утрачивается навсегда. Ярким примером реализации такой угрозы послужила недавняя атака на видеохостинг Rutube, вследствие которой доступ к данному ресурсы был заблокирован на длительное время.

К данному подходу разделения угроз информационной безопасности придерживаются большинство научных исследователей. Тем не менее на современном этапе в научной доктрине предлагается выделение еще одного вида информационных угроз. Е.В. Вострецова, рассуждая по этому вопросу пишет: «Информация не представляется «в чистом виде», на пути к ней имеется хотя бы какая-нибудь система защиты, и поэтому, чтобы угрожать, атакующая сторона должна преодолеть эту систему. Поскольку преодоление защиты также представляет собой угрозу, для защищенных систем будем рассматривать ее четвертый вид — угрозу раскрытия параметров системы, включающей в себя систему защиты»[97]. Любое несанкционированное воздействие на информацию начинается с анализа информационной системы, в которой данная информация хранится. Целью данного анализа является выявление слабых сторон такой информационной системы и подготовки стратегии воздействия на нее. Следовательно, четвертый вид угроз можно охарактеризовать как посредственные угрозы, так как их реализация напрямую не воздействует на защищаемую информацию или информационную систему. Тем не менее, реализация такой угрозы взывает опасность возникновения первых трех «прямых» информационных угроз.

Однако такой подход основное внимание уделяет техническими аспектам информационной безопасности, не принимая во внимание иные ее элементы,

[97]Вострецова Е.В. Основы информационной безопасности: Учебное пособие. 2019. С. 71.

например, полностью игнорируется социально – правовой аспект. Помимо технической составляющей обеспечения информационной безопасности, необходимо выделять и содержание защищаемой информации. Е.О. Напханенко предлагает разделить все информационные угрозы на две большие группы – «угрозы нарушения конфиденциальности, доступности и целостности информации и угрозы нарушения требований к содержательной части информации»[98].

Под угрозами «нарушения требований к содержательной части информации» данный автор понимает «доступ к неподобающему контенту и доступ к незаконному контенту»[99].

К неподобающему контенту относится информации, противоречащая общепринятым нормам морали и нравственности (насилие, призывы к суициду, пропаганду алкоголизма, наркотиков, курения и т.д.). Под запрещенным контентом подразумевается информация, взаимодействие с которой запрещено действующим законодательством РФ. К такой информации могут относиться сведения, содержащие материалы террористического, экстремистского характера, материалы, направленные на разжигание межрасовой ненависти и др.

Возможно разделение информационных угроз на основании критерия «объект информационной безопасности». Согласно данному критерию можно выделить угрозы личности ил угрозы государству.

Угрозы личности или личностные угрозы – это угрозы, объектами которых является информация конкретной личности или группы лиц. К таким угрозам можно отнести различные виды интернет – мошенничества: СМС – мошенничество (SMiShing), vishing, рассылка электронных писем (fishing) и т.д.

Под угрозами государству (или государственным угрозам) понимается спланированные, организованные и глобальные атаки на информационные системы государства, отвечающие за жизнеспособность основных элементов

[98]Напханенко, Е.О. Понятие и классификация информационных угроз в сети Интернет. 2011. С. 127.
[99]Там же.

государства (экономику, обороноспособность, безопасность, экологию и т.д.). Некоторые авторы предлагают включению в данный вид угроз информационные войны, о которых более подробно изложено в следующем разделе.

Следующим критерием может послужить субъект информационной угрозы, на основании которого можно выделить субъективные и объективные угрозы информационной безопасности. К объективным угрозам относятся информационные угрозы, не связанные с волеизъявлением человека, например, стихийные или природные бедствия, повлиявшие на нормальное функционирование систем, направленных на обеспечение информационной безопасности. Субъективные уже угрозы возникают в результате человеческих действий.

Эндрю Конри-Мюррей высказывает необходимость разделения субъективных угроз еще на две, более узкие группы. Данный автор придерживается мнения, что «субъективные угрозы напрямую связаны с деятельностью человека. К ним можно отнести:

– преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей;

– непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в программном обеспечении или в действиях персонала. В рамках этого вида угроз негативный оттенок приобретает термин «социальный инжиниринг» как манипулирование людьми с целью проникновения в защищенные информационные системы предприятий и/или отдельных пользователей»[100].

Отметим, что выше указаны лишь одни из самых распространённых критерий и групп угроз информационной безопасности. В действительности существует множество различных законодательных, стратегических и доктринальных способов квалификация информационных угроз.

[100]Эндрю Конри-Мюррей. Защита конечных пользователей от атак // LAN. 2002. № 11. С. 4.

Таким образом, на основе различных подходов к определению угроз информационной безопасности, можно сделать вывод, что под угрозами информационной безопасности следует понимать совокупность факторов (событий) негативно влияющих или создающих возможность негативного влияния на интересы личности, общества и государства в информационной среде.

Такие угрозы можно разделить на определенные группы в силу различных критериев. Самым распространенным критерием, который используется действующего российским законодательством, является критерий требований, предъявляемых к защите информации. Благодаря такому критерию все угрозы информационной безопасности можно разделить на 4 большие группы. На стратегическом же уровне невозможно использование такого критерия, так как информационная безопасность не ограничивается одной лишь защитой информации. Именно поэтому в Доктрине информационной безопасности Российской Федерации для разграничения информационных угроз закрепляется такой критерий как цель использования информационных – коммуникационных технологиях. Благодаря такому подход возможен охват более широких аспектов информационной безопасности.

2.2. Меры по обеспечению информационной безопасности

В Государственной политике в области обеспечения информационной безопасности закрепляются основные направления деятельности Российской Федерации, необходимые для защиты государственных интересов, интересов общества и личности в информационной сфере. Для успешной реализации данных направлений принимается целый ряд различных мер, которые можно разделить на несколько групп – законодательные, социально - экономические и политические меры.

Для обеспечения охраняемых интересов были приняты соответствующие законодательные акты, необходимые для регулирования обмена, использования, хранения и защиты информации. Государство важную роль

отводит вопросам регулирования защиты персональных данных граждан. Участившиеся нарушения в области конфиденциальности (а именно «сливы» или «утечка») указывают на уязвимость данной области и на необходимость развития механизма защиты персональных данных. Ярким примером являются недавние утечки данных из баз Яндекса, лабораторий Гемотест и Delivery Club. Как следствие сейчас активно обсуждается законопроект, вносящий изменения в Федеральный Закон «О персональных данных». Немаловажную роль играет также защита коммерческой тайны, регулирование которой осуществляется соответствующим федеральным законом. Охрана засекреченных сведений является одним из важнейших государственных интересов, необходимых для обеспечения безопасности страны. Для защиты такого интереса в свое время был принят федеральный закон, направленный на защиту информации, являющейся государственной тайной.

Таким образом на государственном уровне Российской Федерации принята целая серия правовых актов, содержащих в себе меры, направленные на обеспечение информационной безопасности в различных сферах информационного пространства. Данными законами защищаются интересы государства, общества и отдельно взятой личности.

Немаловажную роль играет регулирование вопросов обеспечения информационной безопасности в условиях международного информационного обмена. Для успешной реализации деятельности по данному направлению, в 2008 году был принят Указ Президента РФ N 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»[101]. Данный указ регулирует правила использования информационно – телекоммуникационных сетей, при помощи которых осуществляется передача информации через государственную границу РФ.

[101]О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена : Указ Президента РФ от 17.03.2008 N 351 // КонсультантПлюс : Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

В тексте рассматриваемого Указа сказано, что «подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети «Интернет» не допускается»[102].

Если существует необходимость в осуществлении такого подключения, то оно осуществляется при использовании специальных средств защиты, утвержденных Федеральной Службой Безопасности РФ. Такие средства защиты предписывается использовать государственным органами РФ для обеспечения защиты общедоступной информации при использовании сетей международного информационного обмена. Кроме того, указывается, что использование технических средств при переговорах, где могут обсуждаться сведения содержащие государственную тайну, может осуществляться только при сертификации таких средств.

Для высших органов государственной власти вводится обязанность использовать только такой сегмент сети «Интернет», который предназначен для органов государственной власти РФ и находится в ведении ФСБ. Использование других сегментов сети «Интернет» разрешается только в исключительных случаях.

Таким образом данным указом определяется порядок деятельности органов государственной власти в сетях информационного международного обмена, устанавливается обязанность применения определённых средств

[102]О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена : указ Президента РФ от 17.03.2008 N 351 // КонсультантПлюс : Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

защиты информации и закрепляется роль ФСБ как субъекта, обеспечивающего безопасность сегмента сети «Интернет», используемого органами государственной власти РФ.

1 мая 2022 года был издан новый Указ Президента N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Новым указом выделятся особая группа субъектов под названием «органы организации», перечень которых закреплен в п.1. Итак, согласно данному пункту новый указ действует в отношении «федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации»[103].

На руководителей данных организаций возлагается исполнение обязанности по обеспечению информационной безопасности, в том числе по вопросам связанных с обнаружением, предупреждением и ликвидацией компьютерных атак. Закрепляется обязанность экстренного реагирования на различные компьютерные инциденты. Предписывается создание структурного подразделения, отвечающего за информационную безопасность в соответствующей организации, а также закрепляется комплекс мер необходимых для обеспечения такой безопасности. Правительство РФ обязано составить типовое положение о лице, ответственного за информационную безопасность, и определить организации, в которых необходимо провести проверку уровня защищенности информационных систем. Помимо этого, указ президента возлагает на ФСБ обязанность проверки и мониторинга центров государственных систем, отвечающих за борьбу с компьютерными атаками.

[103]О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента РФ от 01.05.2022 N 250 // КонсультантПлюс : Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

Новым указом регулируется наиболее важная область обеспечения информационной безопасности. В силу участившихся компьютерных атак на структуры и организации, играющие важную роль в функционировании государства, принятие такого указа является своевременной реакцией на изменения условий текущей международной информационной среды.

Анализ иностранных законодательств позволяет сделать вывод о схожести зарубежного подхода к вопросу закрепления законодательных мер обеспечения информационной безопасности.

В Германии ярким примером является закон «О Федеральном управлении информационной безопасности Германии» (BSIG), содержащий основные меры, необходимы для защиты критической инфраструктуры ФРГ и для работы с информацией в целом. Кроме того, данным законом регламентируется порядок взаимодействия с другими публичными и частными организациями по вопросам информационной безопасности.

Для регламентации деятельности, необходимой для обеспечения информационной безопасности в США еще в 2002 году был принят Закон «Об управлении информационной безопасностью» (Federal Information Security Management Act of 2002), регулирующий общие вопросы обеспечения информационной безопасности и закрепляющий перечень основных мер, необходимых для ее обеспечения. Для своевременного реагирования на новые информационные угрозы, в 2021 году был принят Указ Президента США «О совершенствовании национальной кибербезопасности» (improving the national cybersecurity of the United States). Как отмечают в Белом Доме, поводом для принятия данного приказа послужили компьютерные атаки на инфорационные системы SolarWinds, Microsoft Exchange и Colonial Pipeline. К основным мерам, внедряемых данным указом относятся модернизация и внедрение более новых стандартов безопасности, применяемых федеральным правительством, укрепление безопасности программного обеспечения и создание совета по рассмотрению вопросов, касающихся кибербезопасности (Cybersecurity Safety Review Board), в котором будут заседать представители частных компаний и

власти. Основной задачей данного совета является обсуждение крупных происшествий в информационном пространстве с целью выработки рекомендации и стратегий по укреплению информационной безопасности.

Таким образом, такие государства как, США и ФРГ имея стратегические документы, закрепляющие основные цели и задачи государственной политики по вопросам информационной безопасности, реализуют их путем принятия более узких, специализированных законов и правовых актов, содержащих конкретные меры, необходимые для функционирования системы по обеспечению информационной безопасности.

Социально – экономические меры направлены на внедрение новых технологий в государственную деятельность и повышение уровня информационной образованности населения. Создание современной цифровой экономим является важным элементом обеспечения информационной безопасности. Цифровизация всех процессов существенно отражается на уровне защиты информации, что вызывает необходимость создания и внедрения новых цифровых механизмов защиты.

Ярким примером таких мер служит принятая программа «Развитие цифровой экономики России до 2035 года»[104], согласно которой, главными задачами, стоящими перед РФ, являются технологическое лидерство страны и создание эффективной цифровой экономики. Программа закрепляет основные направления государственной политики, а также перечисляются основные меры, необходимые для достижения вышеназванных целей, например, государству необходимо добиться сокращения коррупционного элемента путем минимизирования человеческого фактора в административной системе, оптимизировать налогообложение путем использования интеллектуальных агентов, работающих по схеме smart contracts (умных контракты) и с использованием индивидуального расчета налоговой нагрузки и т.д.

[104]Программа «Развитие цифровой экономики России до 2035 года : распоряжение Правительства РФ от 28.07.2017 N 1632 – р // КонсультантПлюс : Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

Разработка и внедрение собственных информационной технологий является основой стабильного функционирования и развития системы информационной безопасности. Еще в 2020 году Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации было высказана необходимость в ускорении перехода на российское программное обеспечение, применяемое на объектах критической информационной инфраструктуры Российской Федерации. 30 марта 2022 года был издан Указ Президента N 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»[105]. Данный указ вводит запрет на покупку иностранного программного обеспечения с 31 марта 2022 года, а также на запрет использования такого программного обеспечения органами государственной власти на объектах критической информационной инфраструктуры России. Уже сегодня некоторые крупные российские компании используют российское программное обеспечение, например, «Газпромнефть» использует российскую систему «IT4IT», а Ростелеком перешел на систему отечественных разработчиков «Ред Софт». Таким образом наблюдается постепенный отказ от иностранного программного обеспечения в пользу отечественного.

Существенную роль для обеспечения информационной безопасности играет образование населения, так как именно грамотные специалисты являются гарантом стабильной работы механизмов обеспечения информационной безопасности. Одним из аспектов образовательной деятельности является повышение цифровой грамотности. Э.С. Рассаднев, А.А. Осипенко, А.С. Лубянков считают, что «цифровая грамотность – это набор знаний и умений, которые необходимы для безопасного и эффективного использования цифровых технологий и ресурсов Интернета»[106]. Анализ программы «Развитие цифровой экономики России до 2035 года» позволяет

[105]О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации : указ Президента от 30.03.2022 N 166 // КонсультантПлюс : Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).
[106]Рассаднев Э. С., Осипенко А. А., Лубянков, А. С. Цифровая грамотность населения как фактор развития цифровой экономики в России. 2021. С. 76.

сделать вывод, что должное внимание этому вопросу не уделяется. А.Н. Колмыков, согласен, что «вопрос развития компетентности населения в цифровой грамотности не получил должного внимания в программе, следовательно, это влечет риск возникновения проблемы неумения населения регулярно использовать информационные средства или цифровые технологии, которые будут функционировать к 2025 и 2035 гг.»[107].

Во многих странах действуют различные образовательные программы и порталы, направленные на повышение цифровой грамотности населения. Так, например, в Великобритании было создано интернет – сообщество учителей (TES), которое насчитывает более 8 млн пользователей. Н.А. Горелов, В.В. Литун подчеркивают положительный опыт создания такой платформы и отмечают, что она «обеспечивает доступ к учебным материалам, передовой практике обучения, предоставляет возможность обмениваться идеями на интернет-форумах в зависимости от области знаний»[108]. Многие европейские страны (Великобритания, Португалия, Испания и др.) используют программу DIGCOMPFramework, которая содержит основы необходимые для понимания цифровой компетенции. Данная программа также используется для повышения квалификации учителей в рамках развития цифровой компетенции населения.

К сожалению, Россия не занимает лидирующих позиций в области цифровизации экономики. Основная причина отсутствия лидирующих позиций в данной области заключаются в неэффективной работе по повышению цифровой грамотности населения, что является серьезной проблемой, так как для внедрения цифровых технологий необходимы высококвалифицированные кадры.

Политические меры представляют собой принятие определённых политических решений, направленных на развитие систем обеспечения информационной безопасности. К таким мерам можно отнести укрепление сотрудничества в области информационной безопасности.

[107]Колмыков А.Н. Цифровая грамотность населения как ключевое условие развития цифровой экономики. 2019. С. 30.
[108]Горелов Н.А., Литун В.В. Зарубежный опыт обучения населения цифровой грамотности. 2018. С. 347.

Совместная деятельность по решению проблем информационной сферы является эффективным инструментом не только для обеспечения информационной безопасности, но и для укрепления международного сообщества. Существенного развития международного сотрудничества по обеспечению информационной безопасности можно добиться, например, путем создания механизма обмена данных, касательно угроз и инцидентов в отношении объектов критической информационной инфраструктуры. Такой институт позволил бы оказать серьезное влияние на механизмы по предотвращению информационных атак.

Другим направлением укрепления международного сотрудничества является адаптация международного права к вызовам военно – политического характера. Важной проблемой в данной области является отсутствие международно - правовых механизмов, направленных на предотвращение конфликтов, связанных с использованием информационных технологий. Современная модель обеспечения международной безопасности не адаптирована к проблемам использования современных информационно – коммуникационных технологий в военной сфере, что указывает на необходимость скорейшего урегулирования данного вопроса.

Однако реализация вышеназванных перспектив, связанных с укреплением международного сотрудничества встречается с существенными препятствиями, например, высокий уровень недоверия среди стран, политические обстоятельства и противоречия и т.д. В связи с этим такое сотрудничество имеет ограничительный характер.

Для преодоления вышеназванных барьеров все чаще высказываются предложения о сокращении форматов, в которых обязательным условием является согласование государственной политики по определенным вопросам. Иначе говоря, предлагается снизить уровень государственного влияния в вопросах регулирования информационной сферы. Вместо этого предлагается приложить усилия для увеличения количества центров обмена информацией. Примерами таких центров могут послужить ISAC, который был разработан по

коммерческой инициативе и служит для обнаружения, предупреждения инцидентов в области информационной безопасности и устранения их последствий, а также ISO, занимающаяся стандартизацией в различных областях. Это крупные центры, услугами которых пользуются не только частные компании, специализирующиеся на информационной безопасности, но и органы государственной власти различных стран.

Укрепление международного сотрудничества может реализовываться в форме взаимоотношений между отдельными государствами. Как правило результатом такого сотрудничества становится принятие определённого правового или стратегического документа. Ярким примером данной формы сотрудничества является «Соглашения между Правительством Российской Федерации и Правительством Республики Армения о сотрудничестве в области обеспечения информационной безопасности»[109]. Информационное агентство ТАСС анализируя соглашение подчеркивает, что «основными направлениями сотрудничества России и Армении в области информационной безопасности, в частности, станут координация противодействия угрозам в этой сфере, обмен данными в целях выявления, предупреждения, пресечения и расследования правонарушений, связанных с использованием информационно-коммуникационных технологий в террористических и иных преступных целях»[110].

Также важным элементом межгосударственного сотрудничества по вопросам обеспечения с информационной безопасности является борьба с преступностью в информационном пространстве. Определение преступления, совершенного в киберпространстве было закреплено еще в рамках доклада конгресса ООН «По предупреждению преступности и обращению с

[109]О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Армения о сотрудничестве в области обеспечения информационной безопасности : распоряжение Правительства Российской Федерации от 14.04.2022 № 869-р // КонсультантПлюс : Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

[110]Россия и Армения будут сотрудничать в сфере кибербезопсности [Электронный ресурс] // Информационное агентство ТАСС. Официальный сайт.URL: https://tass.ru/politika/14415285?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 15.05.2022).

правонарушителями»[111], в тексте которого оно определяется как «противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ»[112]. В научной доктрине такое явление рассматривается как киберпреступность. Развитие такого нового противоправного элемента и приобретением им трансграничного характера вызывает необходимость сотрудничества государств в данной области. Одной из форм такого сотрудничества является экстрадиция, т. е. выдача лиц, «в отношении которых компетентные органы запрашивающей Стороны ведут уголовное преследование в связи с каким-либо преступлением или которые разыскиваются указанными органами для приведения в исполнение приговора или постановления об аресте»[113] .

Практика экстрадиции в области киберпреступности уже существует. Ярким примером является проведенная в марте 2022 экстрадиция бывшего канадского государственного служащего Себастьяна Вашон-Дежардена в Соединенные Штаты по обвинению в совершении более десяти атак, совершенных при помощи программ-вымогателей, в результате которых были украдены десятки миллионов долларов. Бывшему канадскому государственному служащему были предъявлены обвинения в сговоре с целью совершения компьютерного мошенничества, с помощью программы-вымогателя, известной как NetWalker. В ходе проведения следственных

[111]Доклад конгресса ООН «По предупреждению преступности и обращению с правонарушителями» // Организация Объединенных Наций. Официальный сайт. – 1980. – URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/ RES/53/70&referer=/english/&Lang=R (дата обращения: 15.05.2022).

[112]Доклад конгресса ООН «По предупреждению преступности и обращению с правонарушителями» // Организация Объединенных Наций. Официальный сайт. – 1980. – URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/ RES/53/70&referer=/english/&Lang=R (дата обращения: 15.05.2022).

[113]Европейская конвенция о выдаче // КонсультантПлюс: Справочная правовая система. — URL: http://www.consultant.ru/ (дата обращения: 20.05.2022).

действий у Себастьяна было изъято 28 151 582 доллара, хранящихся криптовалюте.

Другой формой развития сотрудничества в области информационной безопасности является совместная деятельность в рамках международных организаций.

Так информационная безопасность уже давно является одной из центральных тем повестки дня для стран БРИКС. Первое краткое упоминание о важности создания нормативно – правовой регламентации, касающейся международной информационной безопасности и борьбы с киберпреступностью было сделано в декларации, принятой на 3-м саммите БРИКС, в 2011 году в Санье, Китай. Подход БРИКС к информационной безопасности и киберпреступности был затем более подробно раскрыт и конкретизирован в Форталезской декларации, принятой на 6-м саммите БРИКС, состоявшемся в июне 2014 года в Бразилии.

Необходимость сотрудничества в области информационной безопасности и киберпространства получила дальнейшее отражение в Декларации Бразилиа, принятой на 11-м саммите БРИКС 14 ноября 2019 года. В этой декларации также подчеркивалась «важность признанных ООН норм, правил и принципов ответственного поведения государств в области информационных и компьютерных технологий»[114].

По итогам Нью – Делийской декларации XIII саммита БРИКС был одобрен выпуск электронного справочника регуляторных актов стран БРИКС в сфере информационной безопасности (‘e-Booklet of Information Security Regulations in Finance), а также сборник лучших практик по надзору и контрою за рисками информационной безопасности (Compendium on BRICS Best Practices in Information Security Risks: Supervision and Control).

По инициативе Российской Федерации в 2009 г. заключается «Межправительственное соглашение между членами Шанхайской Организации

[114]Декларация Бразилиа по итогам XI саммита государств – участников БРИКС // БРИКС. Официальный сайт. – 2019. – URL: http://www.kremlin.ru/supplement/5458 (дата обращения: 13.02.2022).

о сотрудничестве в области обеспечения международной информационной безопасности»[115]. По мнению В.М. Кулешова и А.В. Тарасенко принятие данного документа свидетельствует, что «на мировом уровне впервые было зафиксировано наличие остро стоящих угроз информационной безопасности, а также определены принципы, методы сотрудничества стран в конкретной сфере»[116].

Анализируя деятельность ШОС в рамках развития систем информационной безопасности, Т.М. Чумаченко отмечает, что «в 2011 г. четыре страны-участницы ШОС (Россия, Китай, Узбекистан, Таджикистан) пошли еще дальше – на глобальный уровень, – представили в ООН свое видение проблем, связанных с международной информационной безопасностью, в разработанных и направленных письмом Генеральному Секретарю ООН Правил поведения государств в области обеспечения международной информационной безопасности, но, этот проект сначала не прошел. Но начало этих инициатив было заложено»[117].

В феврале 2017 года делегация Секритариата ШОС, выступая на Национальном форуме информационной безопасности, представила доклады, содержащие информацию «о совместных усилиях государств-членов Организации в деле обеспечения международной информационной безопасности в регионе своей ответственности»[118].

В 2021 году была принята Душанбинская декларация ШОС, которая подчеркивает увеличение количества угроз в информационной сфере. В связи с этим члены ШОС выступают против милитаризации информационных систем и настаивают на идее создание мирного, открытого, равного и справедливого информационного пространства.

---

[115]Межправительственное соглашение между членами Шанхайской Организации о сотрудничестве в области обеспечения международной информационной безопасности // Шанхайская организация сотрудничества. Официальный сайт. – 2009. – URL: http://rus.sectsco.org/ (дата обращения: 20.03.2022).

[116]Кулешов В.М., Тарасенко А.В. Международная информационная безопасность как вектор развития национальной безопасности России и Германии. 2019. С. 64.

[117] Чумаченко Т.М. Деятельность ШОС по обеспечению международной информационной безопасности. 2017. С. 4.

[118]Там же.

Для достижения такой целей в настоящее время организуются постоянные встречи экспертов стран ШОС по вопросам международной информационной безопасности, на повестке дня которых находятся такие вопросы как как «взаимодействие стран ШОС на площадках ООН, способы повышения эффективности работы Группы, борьба с использованием ИКТ в преступных целях, а также вопросы, связанные с подготовкой предстоящих заседаний ШОС на высшем уровне»[119].

Большой вклад в обеспечение информационной безопасности вносит Организация договора о коллективной безопасности (ОДКБ). Страны участницы данной организации, в том числе Российская Федерация, всегда подчеркивали важность равного взаимодействия в вопросах информационной безопасности и ее обеспечения. В 2020 году Парламентская ассамблея ОДКБ приняла Концепцию борьбы с киберугрозами. Для ее реализации были приняты Модельный закон ОДКБ «Об информационной безопасности»[120] и Соглашение «О сотрудничестве государств - членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности»[121]. В будущем планируется принятие модельного закона «Об обеспечении критически важных объектов информационной инфраструктуры».

Существенную роль в развитии систем обеспечения и защиты информационной безопасности играет НАТО.

Первые задачи по укреплению информационной безопасности были обозначены еще в 2002 году. Действующей стратегическим документом является «Стратегическая концепция НАТО»[122] 2010 года, в которой отмечается необходимость совершенствования способностей по

[119] Эксперты ШОС обсудили вопросы взаимодействия в сфере МИБ // Шанхайская организация сотрудничества. Официальный сайт. – 2021. – URL: http://rus.sectsco.org/ (дата обращения: 20.03.2022).
[120]Модельный закон ОДКБ «Об информационной безопасности» // Организация договора о коллективной безопасности. Официальный сайт. – 2021. – URL: https://odkb-csto.org/ (дата обращения: 12.03.2022).
[121]Соглашение «О сотрудничестве государств - членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности» // Организация договора о коллективной безопасности. Официальный сайт. – 2019. – URL: https://odkb-csto.org/ (дата обращения: 14.03.2022).
[122]Стратегическая Концепция Обороны и Обеспечения Безопасности Членов Организации Североатлантического Договора // NATO. Official website. – 2010. – URL: https://www.nato.int/cps/ru/natohq/official_texts_68580.htm (дата обращения: 12.05.2022).

предотвращению и обнаружению кибератак, а также интеграция механизмов НАТО по борьбе с угрозами информационной безопасности. С 2014 году информационная безопасность стала входить в элемент коллективной обороны, нападению на которую автоматически активирует ст. 5 Североатлантического договора. Начиная с 2016 года, НАТО рассматривает информационное пространство как сферу проведения специальных операций. На официальном сайте НАТО сказано: «С этой целью ведется адаптация учебно-образовательных программ и программ учений НАТО. Центр передового опыта НАТО по совместной киберзащите отвечает за выработку и координацию учебно-образовательных решений в сфере операций по киберзащите в интересах всех органов НАТО во всем Североатлантическом союзе»[123].

В 2020 году были опубликованы два отчета - Киберугрозы и НАТО 2030: Изучение и анализ горизонтов (Cyber Threats and NATO 2030: Horizon Scanning and Analysis) и НАТО 2030: Единство для новой эры (NATO 2030: United for a New Era).

Первый отчет по сути представляет собой сборник статей, в которых анализируется уровень развития систем информационной безопасности потенциальных противников НАТО – России, Ирана и КНДР. Пятая часть данного сборника содержит основные законодательные меры, необходимые для адаптации к новой информационной реальности, например, предлагается ввести усиление экспортного контроля за нематериальными технологиями. Данная мера необходима для регулирования перемещения военных технологических товаров за границу. Аналогичную меру предлагается ввести и для контроля перемещения программного обеспечения.

Второй отчет содержит основные прогнозы данной организации на 2030 год. В число таких прогнозов входит, что Россия станет основным источником угрозы для НАТО. В связи с этим альянсу необходимо продолжать реагировать на угрозы, исходящие от России. К таким угрозам, в частности, относятся и

[123]Роль НАТО в киберпространстве. Вестник НАТО // НАТО. Официальный сайт. – 2019. – URL: https://www.nato.int/docu/review/ru/articles/2019/02/12/rol-nato-v-kiberneticheskom-prostranstve/index.html (дата обращения: 21.04.2022).

«информационные (гибридные)» атаки на демократические институты альянса. В связи с этим НАТО необходимо придерживаться единства и основных принципов альянса, в целях понуждения России к соблюдению норм международного права.

В соглашении между членами Шанхайской Организации «О сотрудничестве в области обеспечения международной информационной безопасности» закреплено более подробное и полное определение информационной войны: «информационная война - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны»[124].

Необходимо также отметить такое явление как информационная война, оказывающая существенное влияние на принятие политических и законодательных мер в сфере обеспечения информационной безопасности.

НАТО рассматривает информационную войну (information warfare) как «операцию, проводимую с целью получения информационного преимущества над противником»[125].

Суть рассматриваемого явления заключается в контроле собственного информационного пространства, защите доступа к собственной информации, приобретении и использовании информации противника, разрушении его информационных систем и нарушении информационного потока. Информационная война не является новым явлением, однако она содержит

[124]Межправительственное соглашение между членами Шанхайской Организации о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] // Шанхайская организация сотрудничества. Официальный сайт. URL: http://rus.sectsco.org/ (дата обращения: 23.04.2022).
[125]MEDIA – (DIS) INFORMATION – SECURITY // NATO. Official website. – 2020. – URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf (дата обращения: 20.04.2022).

инновационные элементы как результат технологического развития, что приводит к более быстрому и масштабному распространению информации.

В связи с текущим кризисом, связанным с ситуацией в Украине, все чаще звучат заявление о разрастающейся информационной войне между РФ и «коллективным Западом». Российской Федерацией был принят ряд мер, направленных на обеспечение информационной безопасности в условиях такой войны. К таким мерам относится принятие 4 марта 2022 года Федерального Закона N 32 ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации»[126], которым вводится уголовная ответственность за распространение ложной информации о действиях вооруженных сил РФ, а также за публичные действия, направленных на дискредитацию использования таких сил. Кроме того, Роскомнадзором был заблокирован доступ к таким ресурсам как «Эхо Москвы», Deutsche Welle, CNN, BBC, телеканал «Дождь» и «Медуза» (признаны инагентами) и др. 21 апреля 2022 года Тверским районным судом г. Москвы холдинговая компания (Meta Platforms Inc[127]) была признана экстремисткой организацией[128]. Компания пыталась оспорить вышеуказанное решение, однако ее апелляционная жалоба была не удовлетворена[129]. В свою очередь Евросоюзом было принято решение остановить вещание таких Российских СМИ как Russia Today (RT) и Sputnik вместе с ее дочерними компаниями, а популярный интернет видеохостинг YouTube блокирует официальные каналы органов государственной власти РФ, государственных СМИ и отдельных политиков.

[126]О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации : федеральный Закон от 04.03.2002 N 32 ФЗ // КонсультантПлюс : Справочная правовая система.—URL: http://www.consultant.ru/ (дата обращения: 20.05.2022).

[127]Признана экстремисткой организацией и запрещена в РФ.

[128]Решение Тверского районного суда г. Москвы от 21.03.2022 по делу N 02-2473/2022 // Судебные и нормативные акты РФ – URL: http://www.sudact.ru (дата обращения: 30.03.2022).

[129]Апелляционное определение Московского городского суда от 20.06.2022 N 33-21933/2022 по делу N 02-2473/2022 // Судебные и нормативные акты РФ – URL: http://www.sudact.ru (дата обращения: 22.06.2022).

Таким образом, государства, в рамках информационной войны, принимают политические решения, направленные на обеспечение информационной безопасности путем принятия существенных мер, направленных на борьбу с недостоверной информацией. Тем не менее, сложность представляет легитимность поставленных целей и соразмерность принятых мер.

Борьба с недостоверной информацией является легитимной целью. Распространение недостоверных сведений может нанести вред государственным интересам. Именно поэтому борьба с такими сведениями играет важную роль. Для реализации такой цели во многих государствах была создана система аккредитации СМИ, с помощью которой обеспечивается поддержание их профессионального уровня. Одним из аспектов такого профессионализма СМИ заключается в перепроверке материалов с использованием различных источников, в целях публикации достоверных материалов. Следовательно, необходима система аккредитации для СМИ.

Проблема видится в способе достижения такой цели, а именно в соразмерности ограничения конституционных прав на выражение мнения, доступа к информации, распространения информации и рассматриваемой борьбы с ложной информацией. В силу публичности и важности характера событий, происходящих в мире, права на свободу выражения мнения и доступа к информации, распространения информации обладают высоким уровнем защищенности. Важнейшим аспектом в данном случае является установление ложного характера информации, блокируемого СМИ. После установление данного характера, каждый случай блокировки СМИ должен быть обоснован невозможностью применения иных мер, с помощью которых возможно достижение вышеназванных целей, например, блокировка конкретного материала, санкции в отношении лиц, распространивших ложную информацию и т.д. Вышеназванный алгоритм должен применяться при проверке законности мер, принятых РФ и иностранными гражданами в отношении СМИ, однако на

практике, к сожалению, в случае политических противостояний законность отходит на второй план или вообще не учитывается.

Вторым важным элементов является увеличение массированных компьютерных атак по объектам критической информационной инфраструктуры. На заседание Совета Безопасности РФ Президент РФ отметил существенное увеличение таких атак. В свою очередь зарубежные страны также отмечают возросшее число атак на информационную инфраструктуру своих государств. Хакер – группа Anonymous объявила о начале кибервойны в отношении Российской Федерации, группировка Killnet также объявила кибервойну многим странам мира. Конечно, действия данных групп нельзя отождествлять с официальными действиями государств, однако такие «кибервойны» все чаще появляются на мировой арене.

Таким образом, все меры, направленные на обеспечения информационной безопасности, разделяются на три большие группы. Законодательные меры принимаются для создание нормативно – правовой базы, необходимой для надлежащего функционирования систем, нацеленных на обеспечение информационной безопасности. Социально – экономические меры призваны обеспечить создание и внедрение цифровой экономики, посредством введения которой будут использоваться новейшие информационные системы, гарантирующие высокий уровень информационной безопасности. Кроме того, такие меры направлены на повышение цифровой грамотности населения, по уровню развития которой Российская Федерация не занимает лидирующих мировых позиций. Политические меры направлены на улучшения взаимодействия государств по вопросам информационной безопасности. Существующая политическая обстановка в информационном пространстве обозначается как информационная война, рамах которой возможно наблюдается принятие существенных ограничительных мер в отношении СМИ, законность принятия которых находится под вопросом.

Заключение

Исходя из вышеизложенного, можно прийти к следующим выводам.

Деятельность, направленная на обеспечение информационной безопасности, является важнейшим элементом национальной безопасности любого государства. История показывает, что развитие информационных технологий неизбежно порождает развитие новых угроз и вызов в отношении благополучного функционирования мирового порядка. Современное общество характеризируется постоянно увеличивающимся уровнем влияния информационной сферы, под которой подразумевается совокупность таких элементов как информация, информационная структура и субъекты,

посредством которых осуществляется формирование, сбор, использование и распространение информации.

Нормативно – правовая регламентация информационной безопасности представляет собой сложную систему взаимосвязанных между собой правовых актов, международных соглашений, стратегических документов и актов частных организаций. Все источники можно разделить на группы по различным критериям – международные и государственные акты, локальные и универсальные, акты обязательного и рекомендательного характера. Большинство универсальных международных актов являются нормами «мягкого права»

Термин «информационная безопасность» в российском законодательстве представляет собой стратегическое определение, не содержащее четких критериев, необходимых для определения данного понятия, но закрепляющее основные направления государственной политики РФ. Для реализации данной политики на государственном уровне принимаются советующие акты. В зарубежном законодательстве в определении информационной безопасности основной акцент сделан на защиту информации. Минусом такого определения является указание только на техническую составляющую информационной безопасности. Такой подход игнорирует иные аспекты информационной безопасности, направленные на защиту интересов личности, общества и государства.

Деятельность по обеспечению информационной безопасности многоаспектна. Одним из таких элементов является создание и использование эффективной системы защиты информации. Выполнение задачи по созданию такой системы включает в себя принятие целого ряда мер, как юридического характера, так организационно – технического и экономического характера. Важную роль в этом играет подготовка специализированных, высококвалифицированных кадров, необходимых для должного функционирования системы обеспечения защиты информации. Достижение данной цели возможно с помощью разработки соответствующих программ

обучения как на национальном уровне, так и на международном. Положительно скажется и создание международных партнерств, направленных на обмен знаниями и опытом, необходимых для повышения цифровой грамотности общества. Для достижения такой цели европейские страны используют локальные цифровые площадки и программы (TES, DIGCOMPFramework и др.) Российская Федерация к сожалению, не уделяет должного внимания проблеме цифровой грамотности.

Деятельность по обеспечению информационной безопасности базируется на определенных принципов, основные из которых закреплен в ФЗ «О безопасности». В доктрине предлагаются дополнительные принципы, содержание и целесообразность которых, однако, вызывает критику.

Информационные угрозы или угрозы информационной безопасности представляют собой главный вызов современному обществу. В доктрине существуют различные квалификации таких угроз. В основе деления всегда лежит четкий критерий, например, РФ в своих стратегических документах использует критерий как цель использования информационных – коммуникационных технологиях. Такой вариант позволяет охватить все аспекты стратегического элемента информационной безопасности Самым распространённым критерием для разделения информационных угроз является критерий требований, предъявляемых к защите информации. Благодаря такому критерию все угрозы информационной безопасности разделяются на 4 большие группы – нарушение конфиденциальности информации, нарушение целостности информации, нарушение доступности информации и раскрытие параметров систем, обеспечивающих защиту информации.

Меры по обеспечению информационной безопасности также разделяются на определенные группы: законодательные, социально – экономические и политические. Каждая группа мер направленна на обеспечение соответствующего аспекта информационной безопасности. Существенные изменения произошли при использовании политических мер. Кризисы, порожденные боевыми действиями в разных частях мира, привели к началу

ведения активных противостояний государств в информационной среде. Многие политические деятели говорят об информационной войне, способы ведения которой взывают вопросы с точки зрения законности.

Многие подходы к международному урегулированию вопросов в области информационной безопасности должны быть пересмотрены, чтобы определить новые векторы развития международного сотрудничества по вопросам обеспечения информационной безопасности.

Список использованных источников

I. Нормативно – правовые акты

1. Хартия Европейского Союза об основных правах (2007/C 303/01) (Вместе с "Разъяснениями..." (2007/C 303/02)) (Принята в г. Страсбурге 12.12.2007) // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 01.05.2022).

1. Европейская конвенция о выдаче (заключена в г. Париже 13.12.1957) (с изм. от 20.09.2012) // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 20.05.2022).

2. Межправительственное соглашение между членами Шанхайской Организации о сотрудничестве в области обеспечения международной информационной безопасности // Шанхайская организация сотрудничества. Официальный сайт. – 2011. – URL: http://rus.sectsco.org/ (дата обращения: 20.03.2022).

3. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Заключена в г. Будапешт 23.11.2001) (с изм. от 28.01.2003.) // «КонсультантПлюс» : Справочная правовая система.— URL: http://www.consultant.ru/ (дата обращения 10.05.2022).

4. Соглашение «О сотрудничестве государств - членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности» // Организация договора о коллективной безопасности. Официальный сайт. – 2019. – URL: https://odkb-csto.org/ (дата обращения: 14.03.2022).

2. О мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза : Директива Европейского Парламента и Совета ЕС от 6 июля 2016 г. (ЕС) 2016/1148 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 01.03.2022).

3. О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, ведения розыскных или судебных действий, или исполнения уголовных наказаний, а также за свободное перемещение таких данных : Директива Европейского Парламента и Совета ЕС от 27 апреля 2016 (ЕС) 2016/680 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 01.04.2022).

4. Решение № 1202 «Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» // ОБСЕ. Официальный сайт. – 2016. – URL:

https://www.osce.org/files/f/documents/e/4/228521.pdf (дата обращения: 13.03.2022).

5. Российская Федерация. Конституция Российской Федерации : принята всенародным голосованием 12. 12. 1993 : с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 02.04.2022).

6. Российская Федерация. Законы. Об информации, информатизации и защите информации : Федеральный закон от 20.02.1995 № 24 – ФЗ : редакция от 10 января 2003 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 12.02.2022).

7. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : федеральный закон от 27.07.2006 № 149 – ФЗ : редакция от 30 декабря 2021 : с изменениями и дополнениями, вступившими в силу 1 января 2022 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 15.03.2022).

8. Российская Федерация. Законы. О безопасности критической информационной инфраструктуры Российской Федерации : федеральный закон от 26.07.2017 № 187 – ФЗ : последняя редакция // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 04.03.2022).

9. Российская Федерация. Законы. О безопасности : федеральный закон от 28.12.2010 № 390 – ФЗ : редакция от 9 декабря 2020 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 15.02.2022).

10. Российская Федерация. Законы. О государственной тайне : закон Российской Федерации от 21.07.1993 № 5485 – 1 : редакция от 11 июня 2021 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 01.01.2022).

11. Российская Федерация. Законы. О коммерческой тайне : федеральный закон от 29.07.2004 № 98 – ФЗ : редакция от 9 марта 2021 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 01.01.2022).

12. Российская Федерация. Законы. О персональных данных : федеральный закон от 27.07.2006 № 152 – ФЗ : редакция от 2 июля 2021 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 15.02.2022).

13. Российская Федерация. Законы. О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации : федеральный закон от 04.03.2022 № 32 ФЗ : последняя редакция // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 20.05.2022).

14. Telekommunikationsgesetz // Bundesministerium der Justiz. Bundesamt für Justiz. Offizielle Webseite. – 2021. – URL: https://www.gesetze-im-internet.de/tkg_2021/BJNR185810021.html (дата обращения: 21.02.2022).

15. Telemediengesetz // Bundesministerium der Justiz. Bundesamt für Justiz. Offizielle Webseite. – 2009. – URL: https://www.gesetze-im-internet.de/bsig_2009/ (дата обращения: 24.04.2022).

16. Informationsfreiheitsgesetz // Bundesministerium der Justiz. Bundesamt für Justiz. Offizielle Webseite. – 2009. – URL: https://www.gesetze-im-internet.de/bsig_2009/ (дата обращения: 24.04.2022).

17. Zweites Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme// Bundesministerium der Justiz. Bundesamt für Justiz. Offizielle Webseite. – 2009. – URL: https://www.gesetze-im-internet.de/bsig_2009/ (дата обращения: 24.04.2022).

18. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik // Bundesministerium der Justiz. Bundesamt für Justiz. Offizielle Webseite. – 2009. – URL: https://www.gesetze-im-internet.de/bsig_2009/ (дата обращения: 24.04.2022).

19. Federal Information Security Management Act of 2002 [Электронный ресурс] // the federal government of the United States. Library of Congress. Official website. – 2002. – URL: https://www.congress.gov/ (дата обращения: 20.04.2022).

20. Российская Федерация. Указы. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 09.09.2000 № ПР – 1895 : последняя редакция // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 01.01.2022)

21. Российская Федерация. Указы. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента РФ от 05.12.2016 № 646 : последняя редакция // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 12.02.2022).

22. Российская Федерация. Указы. О стратегии национальной безопасности Российской Федерации : Указ Президента РФ от 02.07.2021 № 400 : последняя редакция // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 04.03.2022).

23. Российская Федерация. Указы. Об утверждении основ государственной политики Российской Федерации в области международной информационной безопасности : Указ Президента РФ от 12.04.2021 № 213 : последняя редакция // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 15.02.2022).

24. Российская Федерация. Указы. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации : Указ Президента РФ от 01.05.2022 № 250 : последняя редакция // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

25. Российская Федерация. Указы. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного

информационного обмена : Указ Президента РФ от 17.03.2008 № 351 : редакция от 22 мая 2015 // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

26. Российская Федерация. Указы. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации : Указ Президента РФ от 30.03.2022 № 166 : последняя редакция // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

27. Executive Order on Improving the Nation’s Cybersecurity 12 Mai 2021 // The White House. Official website. – 2021. – URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (дата обращения: 24.04.2022).

28. Российская Федерация. Распоряжения. О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Армения о сотрудничестве в области обеспечения информационной безопасности : Распоряжение Правительства Российской Федерации от 14.04.2022 № 869-р : последняя редакция // «КонсультантПлюс» : справочная правовая система. – URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

29. Российская Федерация. Приказы. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» : редакция от 28 мая 2019 : с изменениями и дополнениями, вступившими в силу с 1 января 2021 // КонсультантПлюс : Справочная правовая система.—URL: http://www.consultant.ru/ (дата обращения: 01.01.2022).

30. Резолюция Генеральной Ассамблеи ООН 53/70 от 4 января 1999 г. «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» // Организация Объединенных Наций :

Официальный сайт. – 1999. – URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 12.04.2022).

31. Резолюция A/RES/73/264 от 22 декабря 2018 г. «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» // Организация Объединенных Наций. Официальный сайт. – 2018. – URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 10.04.2022)

32. Декларация Бразилиа по итогам XI саммита государств – участников БРИКС // БРИКС. Официальный сайт. – 2019. – URL: http://www.kremlin.ru/supplement/5458 (дата обращения: 13.02.2022)

33. Модельный закон ОДКБ «Об информационной безопасности» // Организация договора о коллективной безопасности. Официальный сайт. – 2021. – URL: https://odkb-csto.org/ (дата обращения: 12.03.2022)

34. The EU's Cybersecurity Strategy for the Digital Decade // European Commission. Official website. – 2020. – URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade (дата обращения: 12.05.2022).

35. Стратегическая Концепция Обороны и Обеспечения Безопасности Членов Организации Североатлантического Договора (Утв. Главами Государств и Правительств в Лиссабоне 19.11.2010) // NATO. Official website. – 2010. – URL: https://www.nato.int/cps/ru/natohq/official_texts_68580.htm (дата обращения: 12.05.2022).

36. О внесении изменений в Федеральный закон "О персональных данных" и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных : Законопроект от 06.04.2022 № 101234 – 8 // Официальный интернет – портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 20.04.2022).

37. Концептуальные взгляды на деятельность Вооружённых Сил в информационном пространстве // Официальный интернет – портал правовой информации. – URL: http://www.pravo.gov.ru (дата обращения: 20.04.2022).

38. Weißbuch 2016 Deutschland // Bundesministerium der Verteidigung. Offizielle Webseite. – 2016. – URL: https://www.bmvg.de/de/themen/dossiers/weissbuch (дата обращения: 21.03.2022).

39. National cyber strategy of the United States of America 2018 // White House. Official website – 2018. – URL: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 13.04.2022).

40. 2006-2020 **年国家信息化**发展战略 (2006-2020 Nián guójiā xìnxī huà fāzhǎn zhànlüè; The State strategy for the development of informatization for the period from 2006 to 2020) // China government. Official website. – 2006. – URL: https://baike.baidu.com/item /2006-2020%20%E5%B9%B4%E5%9B%BD%E5%AE%B6%E4%BF%A1%E6%81%AF%E5%8C%96%E5%8F%91%E5%B1%95%E6%88%98%E7%95%A5 (дата обращения: 13.04.2022)

41. Доклад конгресса ООН «По предупреждению преступности и обращению с правонарушителями» // Организация Объединенных Наций. Официальный сайт. – 1980. – URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R (дата обращения: 15.05.2022).

42. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach /* COM/2001/0298 final * // European Union. Official website. – 2010. – URL: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:52005DC0389 (дата обращения: 20.04.2022).

43. Концепция Конвенции ООН «Об обеспечении международной информационной безопасности» // Совет Безопасности Российской Федерации.

Официальный сайт. – 2011. – URL: http://www.scrf.gov.ru/security/information/document112/ (дата обращения: 12.04.2022)

II. Специальная литература

44. Арсентьев, М. В. К вопросу о понятии «информационная безопасность» / М. В. Арсентьев // Информационное общество. –1997. – № 4. – С. 50 – 52.

45. Босхамджиева, Н. А. Понятие угрозы общественной безопасности / Н. А. Босхамиджева // Административное и муниципальное право. – 2012. – № 11(59) – С. 40 – 43.

46. Вострецова, Е. В. Основы информационной безопасности : учебное пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург: Изд-во Урал. ун-та, 2019 – 204 с.

47. Гафнер, В. В. Информационная безопасность : учебное пособие в 2 ч. / В. В. Гафнер. – Екатеринбург: ГОУ ВПО «Уральский государственный педагогический университет». – 2009. – Ч.1. – 155 с.

48. Горелов, Н. А., Литун, В. В. Зарубежный опыт обучения населения цифровой грамотности / Н. А. Горелов, В. В, Литун // Экономика труда. – 2018. – № 2. – С. 343 – 350.

49. Жигулин, Г. П. Организационное и правовое обеспечение информационной безопасности: учебное пособие / Г.П. Жигулин. – Санкт Петербург: СПб НИУ ИТМО, 2014. – 173с. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/67451.html (дата обращения: 23.05.2022).

50. Закупень, Т. В. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ / Т. В. Закупень // Информационные ресурсы России. – 2009. – № 4. – С. 28 – 34.

51. Заседание Совета безопасности РФ от 20 мая 2022 года // Совет Безопасности Российской Федерации. Официальный сайт. – 2022. – URL:

http://www.scrf.gov.ru/security/information/document112/ (дата обращения: 20.05.2022).

52. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2021. — 104 с.

53. Иванов, С. В. Правовое регулирование информационной безопасности личности в Российской Федерации / С. В. Иванов // Вестник Екатерининского института. – 2014. – №1 (25). – С. 50 – 56.

54. Идрисов, Х. В. Информационная безопасность как один из элементов национальной безопасности / Х. В. Идрисов // Международный журнал прикладных наук и технологий «Integral». – 2021. – №2. – С. 152 – 162.

55. Информационная безопасность : учебное пособие / В. Н. Ясенев, А. В. Дорожкин, А. Л. Сочков, О. В. Ясенев ; под ред. В. Н. Ясенева. – Нижний Новгород: Нижегородский государственный университет им. Н. И. Лобачевского – 2017. – 198 с.

56. Кулешов, В. М. Тарасенко, А. В. Международная информационная безопасность как вектор развития национальной безопасности России и Германии. / В. М. Кулешов, А. В. Тарасенко // Социально – экономические явления и процессы. – 2019. – № 105. – С. 60 – 70.

57. Колмыков, А. Н. Цифровая грамотность населения как ключевое условие развития цифровой экономики / А. Н. Колмыков // E-Scio. – 2019. – № 3 (30). – С. 29 – 34.

58. Конри-Мюррей, Эндрю. Защита конечных пользователей от атак / Эндрю Конри-Мюррей // LAN. – 2002. – № 11. – С. 45 – 52.

59. Козлова, Н. Ш. Кибербезопасность и информационная безопасность: сходства и отличия / Н. Ш. Козлова, В. А. Довгаль / Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2021. – № 3(286). – С. 88 – 97.

60. Ловцов, Д. А. Лингвистическое обеспечение правового регулирования информационных отношений в инфосфере / Д. А. Ловцов // Информационное право. – 2015. – № 2. – С. 52 – 54.

61. Лопатин, В. Н. Информационное право : учебник / В. Н. Лопатин. – Санкт Петербург: Юридический центр Пресс. – 2005. – 789 с.

62. Мазуров, В. А. Невинский. В. В. Понятие и принципы информационной безопасности / В. А. Мазуров, В. В. Невинский // Известия Алтайского государственного университета. – 2003. – № 2(28). – С. 57 – 63.

63. Мещерякова, А. Н. Сравнение Доктрин ИБ РФ 2000 года и 2016 года» / А. Н. Мещерякова // НвсФ ФГУП «НТЦ «Атлас». – URL: https://www.atlasnsk.ru/news/186/ (дата обращения: 12.04.2022).

64. Правила ответственного поведения государств в информационном пространстве в контексте международной безопасности // Министерство Иностранных Дел Российской Федерации. Официальный сайт. – 2011. – URL: http://www.mid.ru- / (дата обращения: 11.04.2022).

65. Полякова, Т. А. Правовое обеспечение информационной безопасности при построении информационного общества в России : специальность 12.00.14 «Административное право, финансовое право, информационное право» : Автореферат диссертации доктора юридических наук / Татьяна Анатольевна Полякова ; Российская правовая академия Министерства Юстиции РФ, 2008. – 38 с.

66. Программа «Развитие цифровой экономики России до 2035 года» : Распоряжение Правительства РФ от 28.07.2017. № 1632 – р // Справочная правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/ (дата обращения: 10.05.2022).

67. Рассаднев, Э. С. Цифровая грамотность населения как фактор развития цифровой экономики в России / Э. С. Рассаднев, А. А. Осипенко, А. С. Лубянков // Вестник Пермского Университета. – 2021. – № 1(52). – С. 75 – 79.

68. Роль НАТО в киберпространстве. Вестник НАТО // НАТО. Официальный сайт. – 2019. – URL:

https://www.nato.int/docu/review/ru/articles/2019/02/12/rol-nato-v kiberneticheskom-prostranstve/index.html (дата обращения: 21.04.2022).

69. Ромашкина, Н. П. Эволюция политики КНР в области информационной безопасности / Н. П. Ромашкина, В. Г. Задремайлова // Пути к миру и безопасности. – 2020. – № 1(58). – С. 122 – 138.

70. Россия и Армения будут сотрудничать в сфере кибербезопсности // Информационное агентство ТАСС : [сайт]. – 2022. – 19 апр. – URL: https://tass.ru/politika/14415285?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 15.05.2022).

71. Стрельцов, А. А. Содержание понятия «обеспечение информационной безопасности» / А. А. Стрельцов // Информационное общество. – 2001. – № 4. – С. 10 – 16.

72. Урсул, А. Д. Информационная стратегия и безопасность в условиях устойчивого развития / А. Д. Урсул // Организация и методика информационной работы. – 1996. – № 1. – С. 5 – 10.

73. Филатов, В. В. Зарубежный опыт правового регулирования информационной безопасности / В. В. Филатов // Восточно – европейский научный журнал. – 2018. – № 3(31). – С. 69 – 72.

74. Чумаченко, Т. М. Деятельность ШОС по обеспечению международной информационной безопасности / Т. М. Чумаченко // Вестник КазНПУ. – 2017. – № 1(48). – С. 4 – 10.

75. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В. Ф. Шаньгин. – Москва: Издательство «ФОРУМ»: ИНФРА-М. — 2011. — 416 с.

76. Эксперты ШОС обсудили вопросы взаимодействия в сфере МИБ // Шанхайская организация сотрудничества. Официальный сайт. – 2021. – URL: http://rus.sectsco.org/ (дата обращения: 20.03.2022).

77. Яхъева, М. И. Информационная безопасность как составная часть национальной безопасности РФ / М. И. Яхъева // Государственная служба и кадры. – 2020. – № 2. – С. 42 – 44.

78. Glossary of National Institute of Standards and Technology // National Institute of Standards and Technology. Official website. – 2022. – URL: https://csrc.nist.gov/glossary/term/information_security (дата обращения: 13.03.2022).

79. Information security standards ISO/IEC 27000:2018 // International Organization for Standardization. Official website. – 2018. – URL: https://www.iso.org/ru/standard/73906.html (дата обращения: 13.03.2022).

80. Mezhdunarodnoye sotrudnichestvo v oblasti informatsionnoj bezopasnosti [International cooperation in information security] // Министерство Иностранных Дел Российской Федерации. Официальный сайт. – 2019. – URL: http://www.mid.ru- /mezdunarodnaa-informacionnaa-bezopasnost/-/asset_-publisher/UsCUTiw2pO53/content/id/486848 (дата обращения: 10.04.2022).

81. MEDIA – (DIS) INFORMATION – SECURITY // NATO. Official website. – 2020. – URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf (дата обращения: 20.04.2022).

82. U.S. Attorney's Office (Middle District of Florida) // United States Department of Justice. Official website. – 2022. – URL: https://www.justice.gov/usao-mdfl/pr/former-canadian-government-employee-extradited-united-states-face-charges-dozens

III. Судебная практика

1. Постановление Конституционного Суда РФ от 23.11.2017 по делу о проверке конституционности статей 21 и 21^1 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина Е.Ю. Горовенко // Судебные и нормативные акты РФ – URL: http://www.sudact.ru (дата обращения: 01.01.2022).

2. Постановление Конституционного Суда РФ от 06.11.2014 по делу о проверке конституционности статей 21 и 21^1 Закона Российской Федерации «О государственной тайне» в связи с жалобой гражданина О.А. Лаптева //

Судебные и нормативные акты РФ – URL: http://www.sudact.ru (дата обращения: 01.01.2022).

3. Апелляционное определение Московского городского суда от 20.06.2022 N 33-21933/2022 по делу N 02-2473/2022 // Судебные и нормативные акты РФ – URL: http://www.sudact.ru (дата обращения: 22.06.2022).

4. Решение Тверского районного суда г. Москвы от 21.03.2022 по делу N 02-2473/2022 // Судебные и нормативные акты РФ – URL: http://www.sudact.ru (дата обращения: 30.03.2022).

Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Юридический институт
институт
Кафедра международного права
кафедра

УТВЕРЖДАЮ
Заведующий кафедрой
_____ Т.Ю. Сидорова
подпись инициалы, фамилия
« 22 » 06 2022г.

БАКАЛАВРСКАЯ РАБОТА

40.03.01.01 Международное и иностранное право
код – наименование направления

Обеспечение информационной безопасности в сети Интернет: сравнительно – правовой анализ
тема

Руководитель Терешкова 10.06.22 к.ю.н., доцент В.В. Терешкова
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник 10.06.22 М.Д. Чеконов
подпись, дата инициалы, фамилия

Красноярск 2022