МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра гражданского права и процесса

РЕКОМЕНДОВАНО К ЗАЩИТЕ В ГЭК
Заведующий кафедрой
кандидат юридических наук, доцент
_____Краснова Т.В.
«09» декабря 2019 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистра

ОГРАНИЧЕНИЕ ГРАЖДАНСКИХ ПРАВ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА

40.04.01 Юриспруденция
Магистерская программа «Гражданское и семейное право»

Выполнил работу
Студент 3 курса
заочной формы обучения
Некурящих
Илья
Игоревич

Научный руководитель
доктор юр.наук, профессор
Марочкин
Сергей
Юрьевич

Рецензент
доктор юр.наук, профессор
Абдулин
Роберт
Семёнович

Тюмень
2019

Некурящих Илья Игоревич. Ограничение гражданских прав с целью обеспечения безопасности государства: выпускная квалификационная работа магистра : 40.04.01 Юриспруденция, магистерская программа «Гражданское и семейное право» / И.И.Некурящих : науч. рук. С.Ю.Марочкин ; рец. Р.С.Абдулин ; Тюменский государственный университет, Институт государства и права, Кафедра гражданского права и процесса. – Тюмень, 2019. – 101 с.: граф., фот. – Библиогр. список: с. 80-101 (195 назв.).

Ключевые слова: Государственная безопасность, гражданские права, ограничение прав граждан, информационная безопасность.

ОГЛАВЛЕНИЕ…….……..3

ВВЕДЕНИЕ……5

ГЛАВА 1. БЕЗОПАСТЬ ГОСУДАРСТВА КАК ОСНОВАНИЕ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ……..8

1.1. ПОНЯТИЕ И УГРОЗА БЕЗОПАСНОСТИ ГОСУДАРСТВА КАК ОСНОВАНИЯ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ……...….8

1.2. СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА...17

ГЛАВА 2. ПОНЯТИЕ, ПРИНЦИПЫ, СОДЕРЖАНИЕ И ОБЩАЯ КЛАССИФИКАЦИЯ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА……..…24

2.1. ПОНЯТИЕ, ПРИНЦИПЫ И СОДЕРЖАНИЕ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ……...25

2.2. ОБЩАЯ КЛАССИФИКАЦИЯ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ…….....30

ГЛАВА 3. ОГРАНИЧЕНИЯ ГРАЖДАНСКИХ ПРАВ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ…….36

3.1. НЕКОТОРЫЕ ВОПРОСЫ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ……..…36**Error! Bookmark not defined.**

3.2.АНАЛИЗ ЗАРУБЕЖНОЙ ПРАКТИКИ В ОГРАНИЧЕНИИ ГРАЖДАНСКИХ ПРАВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ……42

3.3. СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ……..69

ЗАКЛЮЧЕНИЕ……..….....77

БИБЛИОГРАФИЧЕСКИЙ СПИСОК……80

ВВЕДЕНИЕ

Обеспечение безопасности государства заключается в решении целого ряда задач с целью защиты государства, даже если это не отвечает интересам отдельно взятых граждан и даже отдельных социальных групп. По своей специфики такие меры могут быть административными, организационными, экономическими, политическими, психологическими, правовыми и т.п.

Государство обеспечивает безопасность граждан посредством защиты их жизненно важных интересов. Безопасность может обеспечиваться как путем проведения мероприятий, направленных на его защиту от существующих угроз, так и путем нейтрализации самой угрозы. На наш взгляд, эффективнее представляется вариант устранения угрозы, самого источника опасности.

Во всем цивилизованном мире абсолютная ценность прав человека и подчинения государства интересам граждан является залогом демократического развития общества.

Соответствующее определение юридических границ прав человека является более широким понятием, что определяется следующими факторами:

-интересы (потребности) человека, сбалансированные с потребностями общества;

-мораль, что доминирует в соответствующем обществе в определенное время;

- цель определенного права человека и соответствие ей право реализационной, право обеспечительной и право ограничительной деятельности государства.

С целью избежания злоупотребления властью и волюнтаризма деятельность государства по установлению ограничения прав и свобод человека должна быть регламентированной.

Такие мероприятия являются цивилизованным способом регулирования меры свободы человека в обществе и обусловлены тем, что нормальный процесс функционирования и развития общества порождает ситуации,

требующие от государства правомерного установления ограничения прав человека.

Общей тенденцией при установлении ограничений прав и свобод человека, как считает большинство ученых, является разделение этих ограничений с учетом специфики сферы их действия.

Свобода одного человека должна ограничиваться свободой другого в той мере, в какой это необходимо для равного обеспечения и защиты свободы всех членов сообщества, а государство выступает как гарант такого ограничения[92]. В информационной сфере можно проследить динамику целенаправленного развития, когда мера свободы определяется усмотрением государственной структуры. Зачастую государство пытается оградить общество от той информации, которая, по мнению этого государства, является нежелательной для распространения в обществе. Мы наблюдаем процесс, когда информация, не являющаяся с точки зрения законодательства конфиденциальной и по своей специфике легальна, оказывается недоступной для широких масс.

Попытки государства регулировать доступ к информации в полном объеме в своей основе выражаются в возможности ее получения, а также в контроле источников получения информации. Таким образом, ограничивая от распространения общественно значимую информацию, государство контролирует развитие ситуаций в обществе.

Бесспорно, никто не отрицает присутствие в Интернете нелегального контента, использования информационно-коммуникационных технологий в антигосударственных и противоправных целях. Наличие данного факта не означает, что пользователь не должен иметь возможность пользоваться теми благами, которые предоставляет Всемирная паутина.

Исследование данных вопросов и определило актуальность исследования.

Объект исследования. Объектом работы являются отношения, возникающие в процессе реализации правовых норм, устанавливающих

ограничения прав и свобод граждан с целью обеспечения безопасности государства.

Предмет исследования. Предметом исследования являются положения Конституции Российской Федерации, федеральных конституционных законов, а также других отечественных и зарубежных нормативных правовых актов об ограничениях прав и свобод граждан.

Цель: исследование ограничения прав и свобод граждан в условиях обеспечения безопасности государства.

Для достижения цели исследования были поставлены следующие задачи:

- определить понятие, источники правового регулирования и угрозы безопасности государства как основания ограничений гражданских прав;

- рассмотреть способы обеспечения безопасности государства;

- определить понятие, принципы и содержание ограничений гражданских прав;

- дать общую классификация ограничений гражданских прав;

- исследовать ограничения гражданских прав в сфере информационной безопасности;

- провести анализ зарубежной практики в ограничении гражданских прав в сфере информационной безопасности;

- выработать методы возможного решения сложившихся проблем в правоприменительной практике.

Эмпирическая база – нормативно-правовые акты, которые используются при написании работы Конституция Российской Федерации, Федеральные конституционные законы, а также другие отечественные и зарубежные нормативные правовые акты об ограничениях прав и свобод граждан.

Методологическая основа. При написании работы использованы исследования использованы анализ и синтез, использовались как общенаучные, так и частные методы исследования.

В магистерской диссертации были использованы результаты исследований полученные в результате написания научной исследовательской работа:

Некурящих И.И. Противопоставление безопасности государства и информационной открытости общества // Юрист спешит на помощь. ИГ Юрист. 2019.№1. С.4-8.

Структура исследования. Работа состоит из введения, трех глав, объединяющих в себе семь параграфов, заключения и списка использованных источников.

ГЛАВА 1. БЕЗОПАСТЬ ГОСУДАРСТВА КАК ОСНОВАНИЕ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ

1.1. ПОНЯТИЕ И УГРОЗА БЕЗОПАСНОСТИ ГОСУДАРСТВА КАК ОСНОВАНИЯ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ

Понятие «безопасность государства» содержится в нескольких статьях Конституции Российской Федерации. В частности, ч. 3 ст. 55 предусматривает возможность ограничения федеральным законом прав и свобод человека и гражданина, но только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Президент Российской Федерации, вступая в должность, приносит присягу, текст которой установлен ч. 1 ст. 82, содержащей клятву защищать, в том числе, безопасность государства.

В ряде федеральных законов также содержится указанное словосочетание, но, к сожалению, без расшифровки данного понятия. В Федеральном законе «О безопасности»[90] раскрывается деятельность государства по обеспечению безопасности в целом, куда включены все виды безопасности: и безопасность государства, и общественная безопасность, и экологическая безопасность, и безопасность личности, и иные видов безопасности, предусмотренные законодательством Российской Федерации (ст. 1). Федеральный закон «О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства»[80], используя это словосочетание, в том числе в своем названии, также не объясняет, что понимается под словосочетанием «безопасность государства».

Правовыми средствами обеспечения безопасности на законодательном уровне являются федеральные конституционные законы и федеральные законы. В числе первых можно выделить Федеральные конституционные законы, непосредственно связанные с вопросами обеспечения безопасности: от

30.01.2002 N 1-ФКЗ «О военном положении»[59], от 30.05.2001 N 3-ФКЗ «О чрезвычайном положении»[60] и др. В числе вторых можно упомянуть Федеральные законы от 31.05.1996 N 61-ФЗ «Об обороне»[61], от 12.02.1998 N 28-ФЗ «О гражданской обороне»[62], от 21.12.1994 N 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»[63], от 21.12.1994 N 69-ФЗ «О пожарной безопасности»[64], от 10.12.1995 N 196-ФЗ «О безопасности дорожного движения»[65], от 09.01.1996 N 3-ФЗ «О радиационной безопасности населения»[66], от 21.07.1997 N 116-ФЗ «О промышленной безопасности опасных производственных объектов»[67], от 06.03.2006 N 35-ФЗ «О противодействии терроризму»[68], от 25.07.2002 N 114-ФЗ «О противодействии экстремистской деятельности»[69], от 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[70], от 25.12.2008 N 273-ФЗ «О противодействии коррупции»[71]. Отдельно стоит отметить такие кодифицированные акты, как Уголовный кодекс РФ, Уголовно-процессуальный кодекс РФ, Кодекс РФ об административных правонарушениях.

Необходимо также упомянуть, что в таком основном концептуальном документе, как «О Стратегии национальной безопасности Российской Федерации», утвержденный Указом Президента РФ от 31.12.2015 N 683[91], согласно ее п. 6, под национальной безопасностью Российской Федерации, исходя из текста Стратегии, понимается совокупность внутренних и внешних условий существования личности, общества, государства, обеспечивающих достойную жизнь гражданам, защиту интересов общества, суверенитет народа, исключающих возможность насильственного изменения конституционного строя[91].

Таким образом, в отсутствие четко закрепленного на законодательном уровне понятия «безопасности», сформировывается пробел в праве, что приводит свободному толкованию основополагающего для многих актов понятия.

Таким образом, на доктринальном уровне не выработано единого понятийно-категориального аппарата, который бы четко смог разграничить используемые в современных научных исследованиях понятия «конституционная безопасность», «безопасность личности» и «личная безопасность». Это действительно разноплановые и взаимозависимые категории.

Именно этот признак он предлагает рассматривать в качестве важнейшего критерия разграничения указанных видов безопасности. В научной литературе теоретиками права вопросу классификации ограничений прав и свобод человека посвящено не достаточно внимания. Однако, некоторые ученые в своих трудах поверхностно исследовали этот вопрос. В частности, представитель отраслевой науки конституционного права Б. С. Эбзеев считает, что ограничения прав человека можно разделять на такие виды:

1. ограничение прав и свобод, обусловленные особенностями правового статуса отдельных категорий граждан (должностные лица, военнослужащие) и их отношениями с государством;

2. ограничения общего характера, которые касаются общего конституционного статуса и определяющие допустимые пределы изъятий из основных прав и свобод, и цели, с которыми такие исключения должны быть соразмерными;

3. ограничения основных прав в условиях чрезвычайного положения[183].

Впервые в отечественном праве правовое регулирования института национальной безопасности послужило принятие «Уложение о наказаниях уголовных и исправительных» 1845 г., где одним из отягчающим обстоятельством совершения преступления стала признана угроза посягательства на безопасность государства (п. 8 ст. 135 Уложения).

В настоящее время в Российской Федерации действует огромный массив законодательства в области обеспечения безопасности и ее отдельных видов. В соответствии со ст. 1 Закона о безопасности к таким видам отнесены:

безопасность государства, общественная безопасность, экологическая безопасность, безопасность личности и иные виды безопасности, предусмотренные законодательством Российской Федерации. Таким образом, базовый Закон о безопасности называет лишь ключевые, на взгляд законодателя, виды безопасности, для которых закон определяет принципы и содержание деятельности по их обеспечению.

Надо сказать, что к настоящему времени в нашей стране создана определенная информационно-правовая база для обеспечения координации в сфере обеспечения национальной безопасности, имеются некоторые практические наработки в этом направлении. К примеру, в Федеральном законе «О безопасности», в ст. 6, прямо говорится о координации деятельности по обеспечению безопасности, а в п. 5 ст. 14 предписана координация деятельности федеральных органов исполнительной власти и органов власти субъектов РФ по реализации принятых Президентом РФ решений в области обеспечения безопасности; она возложена на Совет Безопасности РФ. Наряду с изложенным, эта функция продублирована и в п. «б» ст. 4 и ст. 20 Положения о Совете Безопасности Российской Федерации.

В ст. 4 Закона о безопасности отмечается, что государственная политика в области обеспечения безопасности базируется на совокупности скоординированных и объединенных единым замыслом правовых и иных мер, осуществляемых органами власти на основе Стратегии национальной безопасности и других концептуальных, а также доктринальных документов в сфере безопасности. В настоящее время действуют такие концептуальные и доктринальные документы в сфере безопасности, как Доктрина продовольственной безопасности РФ (утв. Указом Президента РФ от 30.01.2010 N 120)[94], Концепция общественной безопасности в Российской Федерации (утв. Президентом РФ 14.11.2013)[95], Концепция противодействия терроризму в Российской Федерации (утв. Президентом РФ 05.10.2009)[96], Стратегия государственной антинаркотической политики до 2020 года (утв. Указом Президента РФ от 09.06.2010 N 690)[97], Стратегия развития Арктической зоны

Российской Федерации и обеспечения национальной безопасности на период Российской Федерации до 2020 года (утв. Президентом РФ 08.02.2013)[97], Национальный план противодействия коррупции на 2016 - 2017 годы (утв. Указом Президента РФ от 01.04.2016 N 147)[99], Стратегия экономической безопасности Российской Федерации на период до 2030 года (утв. Указом Президента РФ от 13.05.2017 N 208)[100], Стратегия экологической безопасности Российской Федерации на период до 2025 года (утв. Указом Президента РФ от 19.04.2017 N 176)[101] и др.

В Стратегии национальной безопасности указано, что «национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности» (п. 6). В Стратегии как составляющие национальной безопасности также указаны международная безопасность (п. 29), военная (п. 33), безопасность в области защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, в области пожарной безопасности (п. 49), продовольственная (п. 54), безопасность в области науки, технологий и образования (п. п. 67 - 69), национальная безопасность в области культуры (п. 76), экологическая безопасность (п. 83). Развитие здравоохранения и укрепление здоровья населения Российской Федерации являются важнейшими направлениями обеспечения национальной безопасности (п. 71)[91].

Основания (условия) введения ограничений прав и свобод в целях защиты основ конституционного строя, обеспечения обороны страны и безопасности государства могут быть:

1) нормативные, которые, в свою очередь, можно подразделить по источнику закрепления на конституционные и законодательные, по отраслевой принадлежности - на конституционно-правовые и отраслевые.;

2) фактические, т.е. совокупность юридических фактов, на основании которых уполномоченный орган государственной власти принимает предусмотренные федеральным конституционным или федеральным законом меры ограничения прав и свобод в отношении граждан и организаций, в том числе иностранных. К ним относятся действия граждан или организаций, которые представляют или могут стать основанием для возникновения угрозы основам конституционного строя, обеспечению обороны страны и безопасности государства.

Способы и средства ограничения прав и свобод в целях защиты основ конституционного строя, обеспечения обороны страны и безопасности государства выступают системообразующим, связующим звеном элементов механизма ограничения прав и свобод в целях защиты основ конституционного строя, обеспечения обороны страны и безопасности государства.

Способы ограничения прав и свобод в целях защиты основ конституционного строя, обеспечения обороны страны и безопасности государства состоят в уменьшении меры дозволенного поведения управомоченного субъекта вплоть до введения запретов во времени, пространстве, по кругу лиц и т.д. или во введении в качестве условий реализации права сопутствующих обязанностей в виде исполнения определенных действий или претерпевания санкций, мер контроля и т.д.

Под информационной безопасностью Российской Федерации согласно Указу Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[92] (Далее- Доктрина информационной безопасности) 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.

Обеспечением информационной безопасности признается осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Состояние информационной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры. В этой связи основными направлениями ее обеспечения являются: повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической инфраструктуры; повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям (п. п. 16, 23 Доктрины).

В ст. 1 Федерального закона от 10.01.2002 N 7-ФЗ «Об охране окружающей среды»[77] (далее - Закон об охране окружающей среды) раскрывается понятие экологической безопасности. Под ней понимается состояние защищенности природной среды и жизненно важных интересов человека от возможного негативного воздействия хозяйственной и иной деятельности, чрезвычайных ситуаций природного и техногенного характера, их последствий.

В соответствии с Основами[104] Государственной политики в области экологического развития РФ на период до 2030 года, утвержденными Президентом РФ 30 апреля 2012 г., разработка основ государственной политики в области экологического развития в России обусловлена

необходимостью обеспечения экологической безопасности при модернизации экономики и в процессе инновационного развития.

Указанные Основы определяют стратегическую цель и основные задачи государства в области охраны окружающей среды и обеспечения экологической безопасности, а также механизмы их реализации. В соответствии с п. 11 Основ основными направлениями обеспечения экологической безопасности являются поэтапное сокращение уровней воздействия на окружающую среду всех антропогенных источников и новая система нормирования допустимого воздействия на окружающую среду (целевым ориентиром является снижение удельных уровней воздействия на окружающую среду в 3 - 7 раз в зависимости от отрасли).

Стратегической целью государственной политики в области экологического развития страны являются сохранение природных систем, поддержание их целостности и жизнеобеспечивающих функций для устойчивого развития общества, повышение качества жизни, улучшение здоровья населения и демографической ситуации, обеспечение экологической безопасности страны. Процесс формирования и реализации экологической политики необходимо внедрять на всех уровнях управления. В принятии и реализации управленческих решений должны участвовать представители не только значимого и приоритетного федерального уровня, но и региональная власть. Механизм обеспечения экологической безопасности, по мнению отдельных ученых, должен включать гуманитарные, экономические и правовые аспекты[135].

Ограничения гражданских прав и безопасность государства непосредственно связаны друг с другом. Появление угрозы безопасности Российской Федерации запускает механизм, который оказывает давление на свободы гражданских прав в угоду эффективности защиты. Нынешнее состояние страны, социально-политическая поляризация российского общества и осложнение международных отношений порождает широкий перечень

возможностей для возникновения внешних и внутренних угроз безопасности государства.

На основании анализа норм законодательства и исследований ученых-теоретиков права, предложена классификация ограничений прав и свобод человека по следующим критериям: в зависимости от юридического статуса право ограничивающего субъекта, целью установления, территорией применения ограничения, степенью соответствия международным стандартам прав и свобод человека, характером нормативной фиксации, степени определенности, по виду прав и свобод человека, определенной категорией субъектов прав и сферой нормативного содержания, способом правового регулирования, стадии правового регулирования, продолжительностью во времени, юридической природой нормативно-правового акта.

1.2. СПОСОБЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА

Обеспечение безопасности государства заключается в решении целого ряда задач с целью защиты государства, даже если это не отвечает интересам отдельно взятых граждан и даже отдельных социальных групп. По своей специфики такие меры могут быть административными, организационными, экономическими, политическими, психологическими, правовыми и т.п.

Государство обеспечивает безопасность граждан посредством защиты их жизненно важных интересов. Безопасность может обеспечиваться как путем проведения мероприятий, направленных на его защиту от существующих угроз, так и путем нейтрализации самой угрозы.

Существенную роль в механизме обеспечения безопасности занимают правовые средства. А.Н. Калюжный отмечает, что «современная система мер по обеспечению национальной безопасности сможет поддерживать институциональные механизмы и ресурсные возможности общества и государства на должном уровне только лишь при наличии совершенных правовых средств»[149].

Многие нормы Конституции РФ направлены на обеспечение защиты как всего населения Российской Федерации, так и отдельных этнических общностей и граждан.

В частности, Конституция РФ устанавливает ответственность при сокрытии фактов и обстоятельств, создающих угрозу для жизни и здоровья людей. Кроме того, в целях обеспечения безопасности государства конституционные нормы прямо запрещают любые формы агитации социальной, расовой, национальной или религиозной ненависти и вражды.

Статья 45 Конституции РФ гарантирует защиту прав и свобод человека и гражданина. Ограничения допустимы лишь в целях обеспечения безопасности. К примеру, ст. 74 Конституции РФ указывает на возможность ограничения перемещения товаров и услуг в целях обеспечения безопасности.

Согласно ст. 69 Конституции РФ гарантируется государственная защита прав национальных меньшинств. Их защита, согласно ст. 71 и 72, отнесена как к ведению Российской Федерации, так и к совместному ведению с субъектами. К совместному ведению отнесены также меры по защите исконной среды обитания и традиционного образа жизни малочисленных этнических общностей. Несмотря на присутствие определенных трудностей экономического, социального, духовного, политико-правового и иного характера, в Российской Федерации накоплен богатый опыт эффективного решения проблем национальных меньшинств[58].

Основные правовые средства обеспечения безопасности государства и мирового сообщества носят системный характер и функционируют на уровнях международного и национального правового регулирования. На международном уровне правового регулирования можно выделить правовые средства глобального, регионального, двустороннего и одностороннего характера. На национальном уровне действуют правовые средства конституционного, законодательного и подзаконного уровня.

Обеспечение безопасности требует со стороны государства определенных мер. В качестве одной из мер государство вынуждено прибегать к

ограничениям прав и свобод человека. Определенная сложность состоит в том, что защита человека, его свободы, интересов практически неотделима от потребности человека в безопасности, что зачастую «развязывает руки» институтам государственной власти.

Рассматривая национальную безопасность через призму защищенности интересов личности, общества и государства от внутренних и внешних военных угроз, К.В. Фатеев приходит к выводу о том, что «системообразующим элементом такой безопасности выступает совокупность национальных интересов России, которые нуждаются в защите военными средствами. Это связано с тем, что, во-первых, определяется круг национальных интересов, для защиты которых государство может пойти на применение военной силы в той или иной форме. Во-вторых, выявляются источники потенциальной военной опасности национальным интересам на текущий период и в перспективе (например, к таким источникам могут быть отнесены действия других государств, направленные на дестабилизацию внутриполитической обстановки в России). В-третьих, указывается, какие факторы государство будет рассматривать в качестве способствующих перерастанию потенциальной военной опасности в непосредственную военную угрозу (например, наращивание группировок войск (сил) у границ России, нарушающее сложившееся соотношение сил, интенсификация оперативной подготовки и др»[176].

Проявление индивида как личности возможно не за пределами организации, а именно в ней, в соответствующих общественных отношениях. Отрицание данного факта способно поставить под удар и личность, и такую корпорацию. Подобные разломы в человеческом сознании, угрозы и опасности, способные привести к возникновению конфликтов, широко используются при ведении информационных и сетевых войн, когда создаются оппозиционно настроенные организации, как реальные, так и виртуальные. Так, например, возможности Интернета широко задействовались и задействуются для

организации так называемых «цветных революций» в Ираке, Ливии, Сирии, Украине.

В связи с федеративным устройством России неизбежно возникает вопрос о допустимости ограничения прав человека законом субъекта РФ. По этому вопросу Конституционный Суд при рассмотрении дела о конституционности ряда нормативных актов субъектов РФ, ограничивающих право граждан на свободу передвижения, сформулировал правовую позицию о том, что права и свободы человека и гражданина могут быть ограничены только федеральным законом (п. 3 мотивировочной части Постановления Конституционного Суда от 4 апреля 1996 г. N 9-П[121]).

Однако данное толкование ч. 3 ст. 55 Конституции расходится с региональной законодательной практикой. Так, Законом Ставропольского края от 29 июля 2009 г. N 52-кз[114], который известен в обиходе как «закон о комендантском часе для несовершеннолетних», в целях предупреждения причинения вреда здоровью детей, их физическому, интеллектуальному, психическому, духовному и нравственному развитию не допускается нахождение лиц, не достигших возраста 16 лет, с 22 часов до 6 часов, а в период с 1 июня по 31 августа - с 23 часов до 6 часов в общественных местах без сопровождения родителей (лиц, их заменяющих) или лиц, осуществляющих мероприятия с участием детей. Аналогичные законы приняты во многих регионах, некоторые из которых предусматривают и более жесткие запреты.

С одной стороны, такие региональные законы ограничивают конституционное право граждан на свободу передвижения, которое согласно указанному решению Конституционного Суда может быть ограничено только федеральным законом. С другой стороны, региональный законодатель действует в соответствии с Федеральным законом от 24 июля 1998 г. N 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»[86] (п. 3 ст. 14.1), который предоставил эту возможность субъектам РФ и тем самым делегировал им полномочия по установлению указанных ограничений.

Подобное делегирование «ограничительных полномочий» получило широкое распространение в различных сферах общественных отношений. Так, например, региональные органы власти вправе устанавливать дополнительные ограничения курения табака в отдельных общественных местах и в помещениях (Федеральный закон от 23 февраля 2013 г. N 15-ФЗ[88]), дополнительные ограничения времени, условий и мест розничной продажи алкогольной продукции (Федеральный закон от 22 ноября 1995 г. N 171-ФЗ[87]). Принятые на этой основе региональные законы неоднократно оспаривались в Верховном Суде, который постоянно отказывал в подобных исках, ссылаясь на установленные федеральными законами дозволения субъектам РФ устанавливать обжалуемые ограничения. Так, Законом Ставропольского края от 3 июля 2007 г. N 23-кз[115] в рамках полномочий, делегированных субъектам РФ Федеральным законом от 29 декабря 2006 г. N 244-ФЗ[89], была запрещена деятельность по организации и проведению азартных игр на территории Ставропольского края. Нормы данного Закона были обжалованы в Ставропольском краевом суде, который отказал в поданном иске. Верховный Суд оставил данное решение без изменения, а кассационную жалобу - без удовлетворения, поскольку, как отмечено в Определении по данному делу, «Закон Ставропольского края о запрете этой деятельности на территории края принят законодателем в пределах полномочий, предоставленных ему Федеральным законом, и, соответственно, не противоречит этому Закону»[77].

Однако установление административных запретов региональными законами считается соответствующим конституционным положениям и в этой связи допустимым, поскольку Конституционный Суд в своем Определении от 1 октября 1998 г. N 145-О[122], исходя из нахождения административного законодательства в совместном ведении Российской Федерации и ее субъектов, разъяснил, что субъекты РФ вправе принимать собственные законы в области административных правонарушений, если они не противоречат федеральным законам, регулирующим те же правоотношения.

С учетом проведенного анализа представляется возможным полагать, что в конституционно-правовой действительности возникло реальное противоречие между правовой позицией Конституционного Суда о том, что права и свободы человека и гражданина могут быть ограничены только федеральным законом, и региональной законодательной практикой, в рамках которой такие ограничения осуществляются повсеместно. Данное противоречие, копившееся годами, образует важную методологическую проблему, которая нуждается в анализе и поиске решения.

Анализируя объекты ограничений и состав субъективных прав, а также элементы правового статуса личности, мы можем выделить систему правовых средств ограничения прав и свобод для обеспечения защиты страны и безопасности государства в зависимости от степени воздействия на субъект ограничения.

1. Введение и применение исходных правовых норм: норм-начал, норм-принципов, норм-дефиниций, определительно-установочных норм.

2. Установление контроля над какой-либо деятельностью лиц, в отношении которых применены или могут быть применены ограничения для выявления оснований введения, применения и соблюдения ограничений.

3. Установление пределов реализации прав и свобод граждан и организаций в конкретных правоотношениях:

- по кругу лиц (субъектному составу правоотношений);

- по юридическим фактам возникновения правоотношений, в которых допустима реализация прав и свобод;

- по обеспечению гарантий исполнения прав и свобод со стороны третьих лиц (ограничение правомочия требования);

- по времени;

- по объекту правоотношения, которым могут быть материальные блага (вещи), нематериальные блага, действия, результаты действий;

- по пространственному критерию;

- по обеспечению гарантий соблюдения прав и свобод со стороны третьих лиц (ограничение правопритязания).

4. Установление обязанностей, сопутствующих реализации права: предварительных, текущих, последующих.

5. Установление материальных (в виде перечня способов защиты) и (или) процессуальных ограничений защиты прав и свобод граждан и организаций с соблюдением принципа недопустимости ограничения судебной защиты.

В качестве примера введения таких ограничений можно привести невозможность ссылаться при рассмотрении гражданского дела на некоторые виды доказательств (ст. 162 Гражданского кодекса РФ).

6. Установление санкций в качестве мер ответственности за совершение противоправных действий, непосредственно не связанных с угрозой основам конституционного строя, обеспечения обороны страны и безопасности государства и (или) ограничений в какой-либо значимой с точки зрения предотвращения вооруженных конфликтов деятельности по признаку наличия совершенного правонарушения и привлечения к юридической ответственности за иное деяние (избирательные цензы, требования по ограничению дееспособности юридических лиц и др.). Примеры таких норм можно встретить в Законе о мерах воздействия.

7. Наделение специальной правосубъектностью, специальной компетенцией, полномочиями для осуществления деятельности, значимой с точки зрения предотвращения вооруженных конфликтов (военнослужащие, военные организации и др.).

Исходя из изложенного, можно определить виды средств ограничения прав и свобод в целях защиты основ конституционного строя, обеспечения обороны страны и безопасности государства:

- по времени действия: постоянные, временные;

- по кругу лиц: общие (индивидуальные и коллективные), специальные (в отношении особых категорий субъектов);

- по условиям применения: в мирное время, в период непосредственной угрозы агрессии, в военное время; в условиях относительной стабильности конституционного строя (в повседневной деятельности), в условиях действия специальных правовых режимов (чрезвычайного положения, военного положения, контртеррористической операции, в боевой обстановке).

Выделенные способы и средства ограничения прав и свобод в интересах обеспечения обороны страны и безопасности государства, основанные на принципах данного правового института, установленных конституционно и в международных правовых актах, применяемые в соответствии с требованиями и нормативно установленными основаниями, выступают системообразующим, связующим звеном между субъектами ограничений прав и свобод личности и организации в интересах обеспечения обороны страны и безопасности государства. Их использование будет способствовать обеспечению безопасности личности, что является условием безопасности общества и государства.

ГЛАВА 2. ПОНЯТИЕ, ПРИНЦИПЫ, СОДЕРЖАНИЕ И ОБЩАЯ КЛАССИФИКАЦИЯ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСУДАРСТВА

2.1. ПОНЯТИЕ, ПРИНЦИПЫ И СОДЕРЖАНИЕ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ

Во всем цивилизованном мире абсолютная ценность прав человека и подчинения государства интересам граждан является залогом демократического развития общества.

Государство, ориентируясь прежде всего на социально-типичные характеристики личности, создает систему взаимных прав и обязанностей, определяющих ее правовой статус. Статус гражданина вытекает из особых правовых связей лица и государства, то есть института гражданства. Однако, рассматривая проблему универсальности прав человека, нельзя обойти вопросы их ограничения. Речь идет не об определении юридических границ естественного права, а об ограничении закрепленных в соответствующих нормативных актах прав человека. Соответствующее определение юридических границ прав человека является более широким понятием, что определяется следующими факторами: интересы (потребности) человека, сбалансированные с потребностями общества; мораль, что доминирует в соответствующем обществе в определенное время; цель определенного права человека и соответствие ей право реализационной, право обеспечительной и право ограничительной деятельности государства[142].

Ограничения играют огромную роль в получении личностью настоящей свободы. Ограничивая в определенной степени свободу каждого индивида, закон обеспечивает ему беспрепятственное использование своих прав, то есть гарантирует ему свободу внутри этих пределов. Свобода каждого человека распространяется только до той границы, от которой начинается свобода других людей. Стремясь установить эти границы, закон содействует тому, чтобы в совместной жизни людей воцарился порядок, основанный на свободе.

Это свойство свободы учитывали еще разработчики французской Декларации прав человека и гражданина от 26 августа 1789.

Российская Федерация, стремясь стать действительно правовым государством, берёт на себя обязанность признания, соблюдения и за щиты прав и свобод человека и гражданина. Это обстоятельство утверждает приоритет прав и свобод личности над государственными интересами. Права человека являются источником постоянного воспроизводства его инициативы, предприимчивости, инструментом саморазвития гражданского общества. Граждане и юридические лица, являясь субъектами гражданского права, вступают в гражданские правоотношения, то есть приобретают и осуществляют права своей волей и в своем интересе. Воля и интерес субъектов гражданского права являются одним из необходимых условий целесообразного и справедливо го функционирования гражданско-правового механизма. Именно воля лежит в основе выбора поведения, достижения интереса субъекта пра ва. Отсутствие воли, какие-либо действия, на правленные на искажение воли, приводят к не действительности гражданско-правовых сделок.

Закрепляя основное значение воли для приобретения и осуществления гражданских прав, ст. 1 ГК РФ (абз. 2 п.2), повторила положения ч. 3 ст. 55 Конституции РФ, в соответствии с которой гражданские права могут быть ограничены федеральным законом только в определенных целях, о которых укажем ниже. Институт ограничения в гражданском праве является мало изученным. Термин «ограничение права» все чаще встречается в правоприменительной практике, используется в науке.

Ограничения гражданских прав установлены и ст. 30 ГК РФ. В силу данной статьи основанием для ограничения прав дееспособного лица является страсть к азартным играм, злоупотребление спиртными напитками или наркотически ми средствами и, как следствие этого, тяжелое материальное положение членов его семьи. Долгое время «страсть к азартным играм» не являлась основанием ограничения дееспособности, но практика показала, что такие действия лица находятся в противоречии с интересами членов его семьи

и влекут непосильные денежные расходы, отражающиеся на благосостоянии семьи. Федеральный закон от 30.12.2012 г. внес изменения в ГК РФ относительно усиления режима ограничения дееспособности граждан, приравняв занятие азартными играми к злоупотреблению спиртными напитками и наркотическими средствами[74].

Здесь ограничение гражданских прав можно рассматривать как одну из санкций, то есть наступление неблагоприятных последствий для таких лиц. Над лицами, ограниченными в дееспособности, назначаются попечители, которые в силу закона получают и расходуют заработок, пенсию и иные доходы гражданина, ограниченного судом в дееспособности, в интересах подопечного Ст. 1 ГК РФ закрепляет основные принципы гражданского права, одним из которых является принцип свободы договора. Свобода договора означает, что граждане и юридические лица самостоятельно решают вопрос о том, с кем и какие договоры заключать, свободно согласовывают их условия. Свобода договора проявляется в различных аспектах: например, это право самостоятельно решать, вступать или не вступать в договор; возможность самостоятельно определять условия договора, контрагента договора; право сторон заключать как предусмотренные, так и не предусмотренные законом договоры, но не противоречащие ему.

Закрепляя принцип свободы договора, ст. 421 ГК РФ предусматривает и ее ограничения. Так, условия договора определяются по усмотрению сторон, кроме случаев, когда содержание соответствующего условия предписано законом или иными правовыми актами. В качестве нормы, ограничивающей свободу договора можно назвать ст. 426 ГК, устанавливающую обязанность заключить публичный договор и право контрагента обязанной стороны обратиться в суд с иском о понуждении заключить договор.

Ст. 429 ГК устанавливает обязанность для лиц, заключивших предварительный договор, заключить и основной договор на тех условиях, которые были предусмотрены предварительным договором. Свобода договора ограничена нормами ст. 250 ГК, устанавливающей преимущественное право

участников общей собственности на покупку доли в праве общей собственности. Императивное требование, содержащееся в пункте 1 статьи 10 ГК РФ, звучит в виде запрета.

Не допускаются осуществление гражданских прав исключительно с намерением причинить вред другому лицу, действия в обход закона с противоправной целью, а также иное заведомо недобросовестное осуществление гражданских прав (злоупотребление правом).

Ограничение основных прав осуществляется как путем прямых запрещений, так и изъятием того или иного правомочия из содержания конкретного права, а также путем установления специального порядка реализации такого права. Отметим, что термин “ограничение” используется как для определения юридических границ прав человека, да и для собственно ограничений последних. Так, И. Ю. Лищина определяет ряд допустимых ограничений прав человека, вызванных объективными причинами или необходимых для существования общества: ограничения, обусловленные уровнем экономического, социального, духовного и культурного развития общества; связанные с конкретным владельцем прав, его экономическими, физическими и другими особенностями; такие, вытекающие из формулы “права человека ограничивают права другого собственника прав”; такие, которые вводит государство (постоянные или временные)[154].

Следовательно, можно сделать вывод, что к собственно ограничений относятся лишь те, что входят к последней из указанных групп, причем в основном временные. Так, к примеру, в. 29 Всеобщей декларации прав человека содержит формулировки постоянных ограничений, необходимых для существования общества, но таких, которые может вводить государство «для удовлетворения справедливых требований морали, общественного порядка и общего благосостояния»[1].

Характеризуя теоретические аспекты ограничения прав человека, можно прийти к выводу, что им присущи определенные признаки. Ограничения представляют собой определенные юридические и фактические последствия в

виде «некомфортных» условий для реализации правовых интересов соответствующих физических и/или юридических лиц, права и свободы которых ущемляются, с одновременным удовлетворением определенных законных интересов субъекта властных полномочий, который ввел эти ограничения, или интересов третьего лица, что заинтересована в введении таких ограничений. Кроме того, в каждом случае ограничения всегда приводят к уменьшению объема разрешенной нормами права поведения или действий субъектов. Вводя ограничения в связи с возникновением чрезвычайных ситуаций, всегда устанавливают законные пределы их реализации, в частности пространственные или срочные.

Правомерное ограничение в условиях возникновения чрезвычайных ситуаций устанавливают только уполномоченные на то субъекты, с соблюдением определенной процедуры, определенной нормативно-правовыми актами. Следующим признаком является то, что ограничение, которое применяется в условиях возникновения чрезвычайных ситуаций, всегда связано с расширением компетенции органов государственной власти или местного самоуправления, ответственные за ликвидацию негативных последствий чрезвычайной ситуации. Причем отметим, что такое расширение происходит за счет уменьшения объема реализации прав, свобод и законных интересов физических и юридических лиц.

Следовательно, можно прийти к выводу, что в любое время и с любого политического режима, ограничения − это расширение полномочий органов государственной власти, а также уменьшение объема прав и свобод и законных интересов физических и юридических лиц.

Кроме того, п. 1 ст. 10 ГК закрепляет положение, в соответствии с которым не допускается использование гражданских прав в целях ограничения конкуренции, а также зло употребление доминирующим положением на рынке. Запрет ограничивать конкуренцию и осуществлять монополистическую деятельность адресован, прежде всего, хозяйствующим субъектам (предпринимателям), занимающим доминирующее положение на товарном

рынке. Конкретные действия, трактуемые как злоупотребление доминирующим положением, названы в Федеральном законе «О защите конкуренции»[73], «О естественных монополиях»[75]. Таким образом, установленные кодексом и законами запреты, не нарушают свободы осуществления гражданских прав, если понимать свободу в осуществлении субъективных гражданских прав как право делать все, что не вредит другим лицам, не нарушает их прав и за конных интересов.

2.2. ОБЩАЯ КЛАССИФИКАЦИЯ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ

С целью избежания злоупотребления властью и волюнтаризма деятельность государства по установлению ограничения прав и свобод человека должна быть регламентированной.

Такие мероприятия являются цивилизованным способом регулирования меры свободы человека в обществе и обусловлены тем, что нормальный процесс функционирования и развития общества порождает ситуации, требующие от государства правомерного установления ограничения прав человека.

В научной литературе теоретиками права вопросу классификации ограничений прав и свобод человека посвящено недостаточно внимания. В частности, представитель отраслевой науки конституционного права Б. С. Эбзеев считает, что ограничения прав человека можно разделять на такие виды:

1. ограничение прав и свобод, обусловленные особенностями правового статуса отдельных категорий граждан (должностные лица, военнослужащие) и их отношениями с государством;

2. ограничения общего характера, которые касаются общего конституционного статуса и определяющие допустимые пределы изъятий из основных прав и свобод, и цели, с которыми такие исключения должны быть соразмерными;

3. ограничения основных прав в условиях чрезвычайного положения[183].

Общей тенденцией при установлении ограничений прав и свобод человека, как считает большинство ученых, является разделение этих ограничений с учетом специфики сферы их действия.

Например, российский теоретик Устинов В. С. предлагает такие виды ограничений прав человека:

1. конституционные и основанные на законах;

2. ограничения, касающиеся всех людей и такие, которые касаются отдельных групп населения (иностранцев, государственных служащих, обвиняемых);

3. ограничения, применяемые в любое время, и те, которые устанавливаются в период военного или чрезвычайного положения относительно определенных видов прав[174].

Указанные виды классификации ограничений прав и свобод человека в целом являются приемлемыми, однако, следов осуществить общетеоретическую классификацию ограничений прав и свобод человека как правового средства.

Следовательно, ограничения прав человека можно классифицировать по следующим критериям:

1. За юридическим статусом субъекта установки: государственные (установленные внутренним законодательством конкретного государства) и международные (установленные международными нормативными актами).

2. С целью установления: сужение возможности осуществления субъективного права человеком или сдерживания антиобщественного поведения.

3. За территорией применения ограничения: международные и внутригосударственные. Международные ограничения прав человека, в свою очередь, делятся на универсальные (например, стандарты ограничения прав, устанавливаемые в рамках ООН) и региональные (например, нормы в области

прав человека, действующих в отношении стран-участниц Совета Европы). Внутригосударственные делятся на общие и локальные, специальные и партикулярные.

Учитывая возможность ограничения прав и свобод человека международными и внутригосударственными актами, необходимо четко учитывать их взаимосвязь и возможные противоречия.

Вместе с тем возникает вопрос о возможности использования международных стандартов прав человека как пределы допустимости ограничения прав и свобод человека.

1. По степени соответствия международным стандартам прав и свобод человека: правомерные и неправомерные.

2. По характеру нормативной фиксации: сужение сферы нормативного содержания и (или) объема прав и свобод человека.

3. По степени определенности: абсолютно определенные (огр - ния-норма имеет определенное содержание и (или) объем прав в законе), относительно определенные ограничения (закон, содержащий норму - ограничение, имеет абстрактный смысл и (или) неопределенный объем прав человека, что ограничиваются).

4. По объему и виду прав и свобод человека: общие (касающиеся всех прав), специальные (устанавливаемые в отношении определенной группы прав), исключительные (распространяются только на одно конкретное право). Специальные ограничения прав человека в свою очередь подразделяются на подвиды: ограничение гражданских, политических прав и ограничения социальных, экономических, культурных прав человека; ограничение абсолютных и относительных прав человека.

5. По кругу лиц и сферой нормативного содержания: общие, специальные (отдельные категории лиц со специальным правовым статусом), единичные ограничения. Европейская конвенция о защите прав человека и основополагающих свобод применяет в ст. 15 общие ограничения (иногда именуемые «генеральными клаузулами»), в ст. 8 специальные ограничения

(ограничения отдельных основных прав, определяющих носителя, сферу нормативного содержания и обстоятельства, допускающие вмешательство органов государственной власти в данную сферу) и в ст. 5 единичные ограничения прав человека (ограничивается одно право)[171].

Общие ограничения применяются в отношении всех прав человека и содержат, как правило, обобщенную характеристику границ допустимости их ограничения. К группе специальных ограничений относятся ограничения отдельных прав человека, определяющих носителя, сферу нормативного содержания и обстоятельства, которые допускают вмешательство органов государственной власти в данную сферу.

Общие и специальные ограничения прав человека соотносятся как «общая» и «особая» части[155]. Как правило, эта общая часть имеет теоретический характер. Конституционные пределы допустимости ограничения основных прав выступают эффективными правовыми средствами, устанавливающих препятствия для произвола публичной власти и предотвращают выхолащиванию истинного значения прав. Особая же часть направлена на анализ отдельных основных прав и позволяет оценивать эффективность реализации конституционно-правовых норм. В свою очередь специальные ограничения прав человека могут делиться на подвиды. Прежде всего следует учитывать существенное различие ограничение 1) основных гражданских, политических прав и 2) основных социальных, экономических, культурных прав.

Ограничение прав и свобод может быть связано с особенностями правового статуса определенных категорий лиц - иностранцев или лиц без гражданства, государственных служащих и/или лиц, которые являются носителями иных публичных полномочий. В зависимости от сферы установки ограничений группы права, ограничиваются, разделяют на абсолютные и относительные права. Как писал в свое время академик Б. М. Топорнин, конституционным правам, реализация которых необходима для общества, а пользование ими не угрожает его существованию «следует приписать высшую

степень абсолютности. Они не должны подлежать отмене или ограничением даже в связи с требованиями чрезвычайного положения»[146]. Поэтому допускается выделение подвидов конкретных ограничений, исходя из абсолютности того или иного конституционного права.

Абсолютные основные права, по общему правилу, не подлежат законодательному ограничению. Они, своего рода, является естественной реакцией на интенсивные неприемлемые ограничения определенных притязаний или полное избавление индивидов отдельных духовных и материальных благ. Считается, что, необходимость защиты прав человека во многих странах стала очевидной после нечеловеческих форм угнетения вследствие революционных вспышек и трагических национальных кризисов. Достичь этого пытались путем сравнительно точной фиксации основных прав в конституции[179]. Конституционное закрепление основных прав заключается в определении списка наиболее ценных благ и интересов индивидов, а также в указании на недопустимость некоторых посягательств на них, исторически наиболее распространенных в государственно-правовой практике.

1.По способу правового регулирования: запрещающие, обязывающие и разрешительные. О. С. Иоффе в свое время выделял так называемые универсальные способы правового регулирования: запрет, разрешение и предписание, которые возможны в любой исторической системе права[145].

2.Наряду с указанными выше позиция, высказанная С. С. Алексеевым, представляется наиболее правильной, поскольку практически согласована с видами правовых норм, которые традиционно делятся на обязывающие, разрешительные и запретительные. Эта позиция является классической, обоснованным и отступать от нее не следует, если основательно не будет аргументировано несоответствие одной или нескольких из этих форм правового регулирования, исходя из специфики ограничений прав человека.

2. За стадией правового регулирования:

правотворческая, правоприменительная и право реализационная. Исходя из юридической силы нормативно-правовых актов, ограничения прав и свобод

человека закрепляются непосредственно Конституцией и законами. При рассмотрении внутригосударственных ограничений прав возникает проблема их разделения на универсальные (действуют на всей территории государства) и локальные (имеющие юридическую силу только на территории отдельных местностей).

3. По продолжительности во времени:

постоянные и временные. Возможность ограничения прав в условиях чрезвычайного положения является общепризнанным фактом и соответствует стандартам прав человека, закрепленным международно-правовыми актами: Международным пактом о гражданских и политических правах (ст. 4); Европейской конвенцией о защите прав человека и основных свобод и Протоколами № 1-11.

Постоянные ограничения закрепляются без указания срока действия. Временные правовые ограничения вводятся на определенный срок или на время действия определенных обстоятельств. При установлении ограничения прав и свобод человека в условиях введения исключительных правовых режимов происходит предоставление больше полномочий государственным органам и сужение содержания или объема прав и свобод человека.

Не может быть ограничен ряд абсолютных прав человека: о равенстве конституционных прав, изменения гражданства, на жизни, достоинства личности, право на неприкосновенность, на жилище, на судебную защиту и так далее. Для нестабильных политических систем использования исключительных правовых режимов, в том числе введение временных ограничений прав и свобод человека, таит опасность их превращения в постоянные правовые средства борьбы с инакомыслием и появления тоталитарных тенденций. Как отмечает А. Шайо, «в начале формирования правового государства любая исключительность создает проблему возврата к тирании, превращение исключения в правило»[179].

4. По юридической природе нормативно-правового акта: законные (установленные законом) и подзаконные (которые устанавливаются подзаконными нормативно-правовыми актами).

Вопрос об установлении ограничений прав и свобод человека в законодательстве имеет как теоретическое, так и практическое значение. Первое заключается в лучшей определенности природы ограничений прав и свобод человека при выяснении этого вопроса и определении действия механизма правового регулирования в отношении таких ограничений. Второе является важным для адекватного установления ограничений прав и свобод человека в национальном законодательстве.

На основании анализа норм законодательства и исследований ученых-теоретиков права, предложена классификация ограничений прав и свобод человека по следующим критериям: в зависимости от юридического статуса право ограничивающего субъекта, целью установления, территорией применения ограничения, степенью соответствия международным стандартам прав и свобод человека, характером нормативной фиксации, степени определенности, по виду прав и свобод человека, определенной категорией субъектов прав и сферой нормативного содержания, способом правового регулирования, стадии правового регулирования, продолжительностью во времени, юридической природой нормативно-правового акта.

ГЛАВА 3. ОГРАНИЧЕНИЯ ГРАЖДАНСКИХ ПРАВ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. НЕКОТОРЫЕ ВОПРОСЫ ОГРАНИЧЕНИЙ ГРАЖДАНСКИХ ПРАВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Развитие интернет-технологий привело к популяризации интернета как инструмента коммуникации и взаимодействия граждан. Рост социальных сетей, возможность неограниченного обмена мнениями и информацией привели к стремительному развитию гражданских сетевых структур, что стало важнейшим инструментом реализации права на доступ к информации, свободы выражения мнения в России и по всему миру.

Свобода одного человека должна ограничиваться свободой другого в той мере, в какой это необходимо для равного обеспечения и защиты свободы всех членов сообщества, а государство выступает как гарант такого ограничения[132]. В информационной сфере можно проследить динамику целенаправленного развития, когда мера свободы определяется усмотрением государственной структуры. Зачастую государство пытается оградить общество от той информации, которая, по мнению этого государства, является нежелательной для распространения в обществе. Мы наблюдаем процесс, когда информация, не являющаяся с точки зрения законодательства конфиденциальной и по своей специфике легальна, оказывается недоступной для широких масс.

Попытки государства регулировать доступ к информации в полном объеме в своей основе выражаются в возможности ее получения, а также в контроле источников получения информации. Таким образом, ограничивая от распространения общественно значимую информацию, государство контролирует развитие ситуаций в обществе.

Из анализа конституционного положения можно сделать вывод, что гражданские права могут быть ограничены как угодно, главное соблюдать

основной принцип - использования федерального закона. Такое понимание теории ограничения права можно признать односторонним и упрощенным, которое приводит к существенному снижению гарантий прав и свобод человека. Что и стало происходить в законодательном поле Российской Федерации.

Нормы, установленные Федеральным законом № 436-ФЗ от 29 декабря 2010 года «О защите детей от информации, причиняющей вред их здоровью и развитию»[83] (Далее – ФЗ №436) и с учетом изменений, принятых Федеральным законом № 139-ФЗ от 28 июля 2012 года «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»[84], направлены на ограничение доступа к вредоносной для несовершеннолетних информации. Законы, на первый взгляд, соответствуют требованиям, заложенным ст. 55 Конституции РФ, но де-факто указанные нормы при их буквальном толковании создают условия для ограничения доступа к информации всех категорий населения, тем самым нарушения права и свободы законопослушных граждан. Возникновение данной проблемы связано с отсутствием в данном законе, четкого, регламентированного и закрытого перечня мест, где распространение данной информации необходимо ограничивать, что, по сути, является коррупциогенным фактором, содержащим неопределенные требования к гражданам и организациям. В результате создается цензурированная экосистема всего Интернета на территории Российской Федерации, где любая информация может быть заблокирована под предлогом того, что даже гипотетически несовершеннолетние могут получить к ней доступ.

Так же коррупциогенные факторы наблюдаются в процедуре экспертизы на наличие запрещенной информации, например, отсутствие или неполнота административных процедур. Это выражено в отсутствии регламентированного перечня информации, которая, согласно ФЗ №436, должна быть ограничена и в отсутствии механизма контроля за проведением экспертиз со стороны граждан, может привести к произволу экспертов и экспертных организаций.

На данный момент действует следующий механизм блокировки: Роскомнадзор, имея решение уполномоченного органа о блокировке того или иного сайта, направляет его владельцу обслуживающего сайт хостинг-провайдера об удалении этой информации. У хостинг-провайдера есть сутки на то, чтобы переслать данное уведомление владельцу сайта. У владельца сайта есть сутки на то, чтобы эту информацию удалить. В противном случае хостинг-провайдер так же в течение дня должен сам удалить данную информацию.

С точки зрения технической особенности взаимодействия провайдера хостинга и владельца сайта, последний может не своевременно получить или даже не получить вовсе уведомления о необходимости удалить страницу с запрещенной информацией. Складывается ситуация, когда владелец вынужден обращаться в суд уже после блокировки, он не может предотвратить ее, и ему приходится доказывать отсутствие запрещенной информации, а не наоборот, что ставит его в неравное положение и нарушает принцип презумпции невиновности.

В октябре 2018 года Госдума приняла в первом чтении законопроект 469143-7[113] о блокировке доступа к так называемым «колумбайн-сообществам», пропагандирующим насилие среди подростков. Законопроект предполагает внесение изменений в Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»[85] (Далее - ФЗ №149), согласно которому блокировке подлежат сайты с информацией, направленной на склонение или иным образом вовлечение несовершеннолетних в совершение противоправных действия, представляющих опасность для их жизни. В то же время законопроект предполагает и серьезные изменения в ст. 15.1 ФЗ №149 относительно механизма блокировки, по большинству видов запрещенного контента. Согласно нынешнему законопроекту, хостинг-провайдер, получив предписание от Роскомнадзора, должен будет «незамедлительно» уведомлять владельца сайта об этом. Тот должен будет «незамедлительно» удалять запрещенный контент, иначе сайт будет заблокирован. Если и этого не произойдет, то

Роскомнадзор заблокирует доступ к соответствующему ресурсу. Всего процесс блокировки занимает от трех дней. Исключение составляет блокировка экстремистской информации, осуществляемая по решениям Генпрокуратуры: она осуществляется «незамедлительно», а владельцы сайтов только после блокировки получают уведомления об этом.

Используемое понятие «незамедлительно» не соответствует действующему законодательству и является коррупциогенным фактором, что выражено в широте дискреционных полномочий (так как присутствует неопределенность сроков) и юридико-лингвистической неопределенности (используются категории оценочного характера)[166].

Следует выделить норму, прописанную в ст. 15.5-15.8 ФЗ №149, позволяющую блокировать IP-адрес сайта, на одной из страниц которого размещена запрещенная информация. Создается цепная реакция, вследствие чего, блокируются десятки не связанных друг с другом ресурсов, являющиеся легальными, с противоположной тематической направленностью информации, но находящихся на одном сетевом адресе. При этом блокировка конкретно одного взятого сайта, включая в себя абсолютно все его элементы, не содержащие противоправный контент, так же нарушает конституционные права граждан.

Так, за пять лет действия ФЗ №436, в различные реестры было внесено около трехсот тысяч страниц. По данным общественной организации «Роскомсвобода», неправомерно было заблокировано (по IP-адресу, что приводит к блокировке сопутствующих сайтов) 3 163 786 сайтов (из них ФСКН-104 643; Роскомнадзором – 334 764; МВД – 677 849 и т.д.)[168].

Данные статистики показывают неэффективность блокировки. Так, за период с 2012 по 2017 гг. число несовершеннолетних потребителей наркотиков увеличилось на 60%[163]. За этот же период количество детской порнографии в Интернете выросло на 63%[150]. Аналогичный рост наблюдается в показателях по числу самоубийств среди несовершеннолетних, на 57%[177].

Федеральный закон от 6 июля 2016 г. №374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» (Далее – ФЗ №374), который предусматривает возложение новых обязанностей на интернет-сервисы, таких как:

1) в течение года хранить и предоставлять по запросу факты приема, передачи и обработки любых сообщений и сведения о пользователях;

2) в течение шести месяцев – всю переписку пользователей, включая передаваемые по сети файлы;

3) предоставить «ключи», необходимые для декодирования принимаемых электронных сообщений, если сервисом используется шифрование.

ФЗ №374, хоть и был направлен на защиту государства и граждан от терроризма, но значительно ограничил права и свободы человека и гражданина, предусмотренные частями 1 и 2 статьи 23, частью 1 статьи 24, статьи 28, частью 4 статьи 29 Конституции РФ, при этом гражданам не дана независимая, объективная, общественная оценка, которая могла подтвердить или опровергнуть результативность предпринятых на основании законодательных мер по борьбе с терроризмом. Таким образом, закон не отвечает критериям, разработанным ООН, и частям 2 и 3 статьи 55 Конституции РФ.

9 мая 2017 г. был принят Указ Президента РФ №203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[93], одним из основных принципов которого является «приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий». Для развития Интернета в России предлагается отстаивать суверенное право государства определять информационную, технологическую и экономическую политику в национальном сегменте Сети, а также исключить анонимность и безответственность пользователей.

Реализация Стратегии уже началась. 1 ноября 2017 г. вступили в силу поправки в Федеральный закон «Об информации, информационных технологиях и о защите информации», обязывающие администраторов VPN и подобных сервисов под угрозой блокировки ограничивать доступ к запрещенной в России информации («закон о запрете VPN»). В течение недели после вступления в силу закона не менее семи сервисов заявили об отказе сотрудничать с Роскомнадзором и вмешиваться в трафик клиентов[167]. А также было принято постановление Правительства Российской Федерации от 27.10.2018 № 1279 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями»[107]. Согласно данному постановлению, мессенджеры должны проверять информацию о номере пользователя у его мобильного оператора. Для этого мессенджер направляет запрос оператору, а тот должен провести проверку и ответить в течение 20 минут. Если номера в базе оператора не окажется или оператор не ответит, мессенджер не зарегистрирует пользователя. Если же пользователь, уже прошедший проверку, позднее изменит сведения о себе или сменит номер телефона, то ему нужно будет пройти процедуру заново.

3.2. АНАЛИЗ ЗАРУБЕЖНОЙ ПРАКТИКИ В ОГРАНИЧЕНИИ ГРАЖДАНСКИХ ПРАВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОТИ

Права человека представляют собой фундамент современного правового государства. На постиндустриальном этапе развития защита прав человека приобретает особый характер. Совершенствование информационно-коммуникационные технологий сопровождается расширением возможностей их недобросовестного использования, которое создает угрозы информационной безопасности и может приводить к нарушениям прав человека. В связи с этим возникает проблема соотношения информационной безопасности и прав человека, прежде всего, права на неприкосновенность частной жизни

Большинство государств отреагировало на возросшие в последнее время угрозы национальной безопасности путем расширения полномочий органов власти по доступу к личной информации, ее сбору и обработке, которые в настоящее время не ограничены какими-то отдельными категориями информации. При этом в различных государствах подходы к обеспечению соразмерности принимаемых мер по обеспечению национальной безопасности также могут отличаться.

В государствах с демократическими правовыми режимами, как правило, установлен приоритет прав человека перед обеспечением национальной безопасности[143]. Такой приоритет выражается в том, что меры по обеспечению национальной безопасности, связанные со сбором и обработкой соответствующей информации, принимаются при соблюдении специальной процедуры, которая обеспечивает их соразмерность возникающим угрозам. В основе данного подхода лежат положения Конвенции 1950 г., в которой определены условия ограничения права человека на неприкосновенность частной жизни — «установление ограничения только законом» и «необходимость в демократическом обществе». Ограничение должно соответствовать целям его установления. Это позволяет не только определить целесообразность или обоснованность установления или применения подобного ограничения, но также оценить возможность эффективного достижения тех же целей в отсутствии ограничения права или его меньшем ограничении.

Для своевременного выявления фактов несоразмерности ограничений прав человека угрозам информационной безопасности и последствиям их проявления могут быть созданы специализированные государственные органы и уполномоченные по правам человека, подконтрольные представительной власти. Как отмечают в зарубежной литературе, «обеспечение неприкосновенности частной жизни не должно ограничиваться тем, что законодатели, судьи и государственные служащие уделяют ей достаточно внимания. Они также должны обеспечить постоянный контроль, чтобы

убедиться, что неприкосновенность частной жизни может играть важную роль в качестве противовеса перед лицом новых угрожающих событий»[144]. В связи с этим Европейский суд по правам человека указывает, что «надзор за мерами наблюдения может осуществляться на трех этапах: когда наблюдение санкционировано, во время его проведения и после того, как оно закончилось. В процессе надзора ценности демократического общества должны соблюдаться как можно более добросовестно...»[85].

Изучение практики европейских стран в построении личных моделей правового обеспечения информационной безопасности, противодействия киберугрозам, а также анализ ряда международных правовых документов позволяет нам резюмировать об отсутствии единой модели национальной системы правового обеспечения информационной безопасности.

Анализ, оценка и использование позитивных достижений европейских стран имеют важное значение при построении системы обеспечения информационной безопасности в РФ, поскольку, как отмечают В. Шатун и О. Гладун [182], события последних лет в нашем государстве показали неспособность власти адекватно противостоять информационным войнам, поскольку проблемы информационной политики до сих пор не решены на должном уровне.

Вопрос относительно условных границ Центральной Европы пока остается дискуссионным. Традиционно к странам Центральной Европы относят Германию, Лихтенштейн, Австрию, Швейцарию и некоторые другие. Впрочем, де-факто к ним относятся и участники Вышеградской группы – Венгрия, Польша, Чехия и Словакия[198], а также часть стран Балканского полуострова. Несмотря на то, что вопросы информационной безопасности в странах внеблокового статуса целесообразно рассмотреть отдельно, пока сосредоточимся на обеспечении информационной безопасности в Германии, Польше, Венгрии и Хорватии[166].

Прежде всего заметим, что Федеративная Республика Германии, Венгерская Республика, Республика Польша и Республика Хорватия являются

членами Организации Североатлантического договора и Европейского Союза. Соответственно, на них распространяются стандарты этих международных организаций по информационной политики и обеспечения информационной безопасности. Это, в частности, стандарты НАТО по защите информации, изложенные в Документе СМ (2002) 49 «Безопасность в Организации Североатлантического договора (НАТО)»[10], официальная политика НАТО в сфере киберзащиты[24], стратегическая концепция кибербезопасности, сформулированная на Лиссабонском саммите[25] и уточнена по результатам Варшавского саммита[26], и др.

Активную политику в сфере обеспечения информационной безопасности проводит не только НАТО, но и ЕС, который сегодня объединяет развитые страны, которые ощутимо влияют на международные отношения, устанавливая нормы и стандарты поведения государств в политической, экономической, социальной, информационной и других сферах. 1991 года было разработано «Европейские критерии безопасности информационных технологий», где, в частности, определены задачи обеспечения информационной безопасности, а именно:

• защита информационных ресурсов от несанкционированного доступа с целью обеспечения конфиденциальности;

• обеспечение целостности информационных ресурсов путем их защиты от несанкционированной модификации или уничтожения;

• обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

В 1996 году стандарты европейской информационной безопасности было воплощено в «Единых критериях безопасности информационных технологий»[31], где применена модель триады CIA (CIA Triad), которая предусматривает следующие основные характеристики информационной безопасности:

1) конфиденциальность;

2) целостность;

3) доступность[159].

В документе Европейской Комиссии «Сетевая и информационная безопасность: европейский политический подход» (2001 г.), определены базовые принципы Сообщества к проблеме обеспечения информационной безопасности. Терминологическое соединение «сетевая и информационная безопасность» трактуется как способность сети или информационной системы сопротивляться случайным событиям или злонамеренным действиям, представляющим угрозу доступности, подлинности, целостности и конфиденциальности данных, хранящихся или передаваемых, а также услуг, предоставляемых через эти сети и системы[30].

Упомянутый документ определяет следующие приоритетные направления европейской политики обеспечения информационной безопасности:

-повышение осведомленности пользователей о возможных угрозах при пользовании коммуникационными сетями;

- создание европейской системы предупреждения и информирования о новых угрозах;

- обеспечение технологической поддержки;

- поддержка рыночно ориентированной стандартизации и сертификации;

-правовое обеспечение, приоритетами которого является защита персональных данных, регламентация телекоммуникационных услуг и противодействие киберпреступности;

- укрепление информационной безопасности на государственном уровне путем внедрения эффективных и совместимых средств обеспечения информационной безопасности и поощрения использования государствами-членами электронных подписей при оказании государственных онлайн услуг и т. п.;

-развитие международного сотрудничества по вопросам информационной безопасности. Во всех без исключения странах ЕС вопросам правового обеспечения информационной безопасности уделяется особое внимание.

При этом первостепенное значение приобретают вопросы противодействия киберугрозам, которые являются составляющими процесса обеспечения информационной безопасности. С 1999 года реализуются программы «Безопасный Интернет» (Safer Internet), в рамках которых осуществляются мероприятия, направленные на борьбу не только с вредным контентом, но и с опасным поведением в сети. Процесс формирования европейской глобальной системы правового обеспечения информационной безопасности имеет длительный характер. Еще в 2007 году Европейская Комиссия приняла документ «На пути к общей политики в сфере борьбы с киберпреступностью»[28].

В данном документе, хотя и на уровне декларации, определено киберпреступления как криминальные действия, совершенные с использованием электронных коммуникационных сетей и информационных систем или против таких сетей и систем, которые включают:

-традиционные формы преступления (мошенничество и подделки в электронных коммуникационных сетях и информационных системах);

-публикацию незаконного контента в электронных медиа;

-специфические преступления в электронных сетях (атаки на информационные системы, хакерство и тому подобное)[29].

Несколько позже, в 2009 году в Сообщении Европейской Комиссии «Защита Европы от крупномасштабных кибератак и разрушения: усиление уровня подготовленности, безопасности и устойчивости» были определены главные вызовы и проблемы, которые требуют первоочередного реагирования со стороны стран ЕС, а также обозначило основные меры по усилению безопасности и способности европейской критической информационной инфраструктуры противостоять внешним воздействиям [378]. Согласно данного документа вызовами безопасности информационной безопасности стран ЕС являются:

• некоординированные национальные подходы к безопасности информационных инфраструктур, снижает эффективность национальных мер;

• отсутствие на европейском уровне партнерства между государственным и частным секторами;

• ограниченные возможности раннего предотвращения и реагирования на опасные инциденты, обусловленные неравномерностью развития систем мониторинга и оповещения об инцидентах в странах-членах, неразвитостью межгосударственного сотрудничества и обмена информацией относительно этих проблем;

• отсутствие международного консенсуса в отношении приоритетов в реализации политики защиты критической информационной инфраструктуры.

Кроме указанного, важным аспектом правового обеспечения информационной безопасности в рамках ЕС является вопрос информационной открытости органов государственной власти стран-участниц. Системообразующим тезисом данного аспекта является: «... общепризнано, что демократическая система может функционировать наиболее эффективно только в случае, когда общественность полностью проинформирована «[152]. В данном ракурсе следует также сослаться и на рекомендации Совета Европы № R(81)19 «О доступе к информации, находящейся в распоряжении государственных органов».

В данном документе отмечено, что для обеспечения адекватного участия всех в общественной жизни необходимо обеспечить, с учетом неизбежных исключений и ограничений, доступ общественности к информации, находящейся в распоряжении государственных органов всех уровней [7]. Первоочередное значение здесь приобретают вопросы защиты персональных данных. По этому поводу, в резолюции Генеральной Ассамблеи ООН «Право на приватность в цифровую эпоху» от 18 декабря 2013 года определен глобальный и открытый характер Интернета и стремительное развитие в сфере информационных и коммуникационных технологий как движущей силы для ускорения прогресса на пути к развитию в различных формах.

В документе подтверждено, что «те же права, что люди имеют в офф-лайн режиме, должны также быть защищены онлайн, в том числе право на

приватность» [8]. Принципы защиты персональных данных в правовой практике стран ЕС можно свести к такому:

-приоритетность права лица распоряжаться своими персональными данными;

- использование персональных данных без разрешения владельца влечет ответственность в соответствии с законодательством;

-для любого, кто осуществляет пользование персональными данными физических лиц с их разрешения, установлена ответственность в случае умышленного разглашения этих данных третьим лицам (кроме случаев, когда на это дано разрешение)[134].

Несмотря на упомянутые документы ЕС о защите персональных данных, основным среди них следует считать директиву 95/46/ЕС «О защите физических лиц в контексте обработки персональных данных и свободного обращения таких данных»[5]. В нем декларируется стремление к свободному перемещению информации между странами-членами ЕС и одновременно предоставляются гарантии защиты основных прав граждан, к которым относится и право на неприкосновенность личных данных и их защиту от третьих лиц. Директива ЕС обязывает каждое государство-члена принять свои национальные законы о защите частных данных, которые соответствовали бы рекомендациям OECD 1980 года.

Среди этих рекомендаций стоит отметить «Принцип гарантированной безопасности N11»[194], который требует, чтобы персональные данные были защищены разумными средствами безопасности от таких угроз, как потеря или несанкционированный доступ, разрушение, использование, модификация или раскрытие». Обязательные для стран-членов ЕС новые правила защиты персональных данных (GDPR), которые принято 14 апреля 2016 года, вступают в силу в 2018 году. Эти правила будут распространяться не только на европейские компании, но и на субъектов других стран, которые предлагают товары и услуги в ЕС. В документе пересмотрены гражданские права пользователей, ответственность за сохранность данных, а также введены

некоторые ограничения перемещения данных между странами. Следует констатировать, что страны ЕС сформировали « в определенном смысле слаженную систему защиты информации»[6], но в то же время каждая страна имеет свои законы, положения, Инструкции по урегулированию вопросов информационной безопасности.

Такая, для Германии характерна детальная нормативно-правовая разработка системы разных видов информации с ограниченным доступом, четкие формулировки их определений в федеральном законодательстве. К примеру, согласно закону «О проверке безопасности» [41] секретной информацией считаются факты, изделия и сведения, независимо от формы их представления, которые в государственных интересах должны храниться в тайне и которым предоставлен государственным органом или по его поручению степень секретности, который соответствует необходимому уровню защиты:

- «совершенно секретно»;
- «тайно»;
- «конфиденциально»;
- «для служебного пользования».

К системе секретной информации относится государственная тайна (информация с грифом «совершенно секретно» и «секретно») и ведомственная тайна (информация с грифом «конфиденциально» и «для служебного пользования»), охрана которых, в отличие от других видов тайн, касающихся конфиденциальной сферы частных лиц, обусловлена интересами внешней безопасности государства. В частности, особенно важной и подлежащей особой защите считается конфиденциальная информация об этническом происхождении, политических взглядах, религиозных и философских убеждениях, членстве в объединениях, здоровье и половой жизни физических лиц. В октябре 1997 года в Германии принят Акт защиты информации в телекоммуникациях (TDPA)[42].

Согласно его общих принципов сбор, обработка и использование информации допускается лишь в случаях, когда это разрешено законом или осуществляется по согласию пользователя. Информация может быть собрана, обработана или использована только отдельно для разных услуг, в которых нуждается один и тот же пользователь, причем согласие последнего не является условием для оказания услуг. Кроме того, с 2005 года в Германии действует так называемый «Акт о свободе информации», который регламентирует вопросы доступа к ней[43].

Надзор за выполнением положений этого нормативного акта возложена на комиссара по защите информации и персональных данных. В стране с 1990 года действует также закон о доступе частных лиц и исследователей к архивам «Штази» – службы безопасности бывшей ГДР[44]. Федеральная служба информационной безопасности (BSI) является главным органом, на который возложены обязанности по обеспечению информационной безопасности страны. BSI входит в Федерального министерства внутренних дел, которое, среди других функций:

• обеспечивает внутреннюю безопасность и защита конституционного строя Германии;

• осуществляет борьбу с терроризмом, экстремизмом, шпионажем и саботажем.

Согласно закону «О Федеральное ведомство безопасности информационных систем» BSI собирает и оценивает информацию относительно угроз кибербезопасности государства, выявляет новые типы кибератак, анализирует соответствующие контрмеры[45].

На BSI также возлагается выполнение следующих функций во взаимодействии с НАТО и ЕС:

• оценка риска внедрения информационных технологий;

• разработка критериев, методов и испытательных средств для оценки степени защищенности национальных коммуникационных систем;

• проверка степени защищенности информационных систем и выдача соответствующих сертификатов;

• выдача разрешений на внедрение информационных систем в важные государственные объекты;

• осуществление специальных мер безопасности информационного обмена в государственных органах, полиции и др;

• консультирование представителей промышленности по вопросам информационной безопасности. Кроме того, ведомство осуществляет меры по пропаганде необходимости обеспечения информационной безопасности[197].

С целью оптимизации оперативного сотрудничества между всеми государственными учреждениями и улучшения координации мероприятий по противодействию кибератакам в ФРГ на базе Федерального ведомства безопасности информационных систем создан национальный центр киберзащиты (NCAZ), который непосредственно взаимодействует с другими субъектами кибербезопасности страны, в том числе с частным сектором, странами-партнерами по ЕС, НАТО, а также международными организациями [153].

Вопросами обеспечения информационной безопасности Германии в рамках своей компетенции занимаются также Федеральное бюро защиты конституции (BFV) [188] и Управления информационных операций, создано в 2009 году в структуре бундесвера через массированные атаки на вычислительные сети государственных структур ФРГ в феврале 2009 года.

В конце 2010 года в рамках реализации концепции киберзащиты в структуре командования бундесвера окончательно завершено также формирование подразделения информационных и компьютерных сетевых операций, которое с 5 апреля 2017 года функционирует как «силы кибернетического и информационного пространства Германии». В задачи указанного подразделения входит, в частности:

• разработка новых методов кибератак;

• проникновение в компьютерные сети иностранных государств и организаций с целью получения разведывательных данных;

• проведение операций деструктивного воздействия на сети и автоматизированные системы или блокирования их работы [189].

Анализ открытых источников по политике информационной безопасности Германии сдает позволяет сделать нам вывод, что среди приоритетов противодействия киберугрозам, Германия избрала тактику так называемой «активной обороны». Выделение наступательной составляющей информационного противоборства и создания соответствующей отдельной структуры, по оценкам немецких экспертов, адекватным ответом на современные угрозы информационной безопасности Германии. Подобная тактика обеспечения информационной безопасности успешно действует и во Франции, где 17 июля 2014 года на уровне законодательного акта определено глобальную политику безопасности информационных систем[190].

Данным правовым актом установлены правила защиты государственных информационных систем, и приоритетный механизм противодействия киберугрозам на уровне государства. Несколько позже, а именно 27 марта 2015 года, вышел Декрет № 2015-351, где правительство Франции сформулировал новые положения безопасности информационных систем операторов отраслей, роль которых имеет критическое значение для жизнедеятельности нации[196].

Приведенные выше законодательные шаги ярко подтверждают, что в странах Центральной Европы вопросам информационной безопасности уделяется особое внимание. Что касается подобной практики наших ближайших соседей, в частности Польши, отметим, национальная информационная политика Республики Польша концептуально ориентирована на развитие свободного открытого общества, обеспечение основополагающих прав человека и гражданина, внедрение концепции свободного трансграничного оборота информации, создания независимых и плюралистических СМИ.

Правовым воплощение польской концепции информационной безопасности являются принятые в 1990-х годах «Закон о почте и телекоммуникациях», «Закон о телевидении и радиовещании», «Закон о государственные отношения с римской католической церковью в Республике Польша», где определены направления информационной политики, устанавливаются технологические стандарты информационной связи, формы привлечения иностранных инвестиций (33%-49% зарубежного капитала), лицензирования информационной деятельности. Отдельно выписаны права церкви на информационную деятельность, учитывая значительное влияние клерикальной информации на политические приоритеты и нравственность польского общества[191].

Основные функциональные полномочия в обеспечении кибернетической безопасности Польши возложена на Агентство внутренней безопасности (ABW). В 2013 году при участии данного органа разработана Стратегия кибербезопасности Польши и создан при Министерстве национальной обороны Центра криптологии, на который возложена задача по защите информации, кибероборонь и проведение наступательных кибероперацій[9]. ABW также сформировало правительственную команду реагирования на компьютерные инциденты (CERT) [11], главной задачей которой является обеспечение и развитие возможностей органов государственного управления по защите от киберугроз.

В частности, это касается защиты от атак на инфраструктуру, которая состоит из ИТ-систем и компьютерных сетей, нарушение работы или разрушение которых может в значительной степени угрожать жизни и здоровью людей, национальным богатствам и окружающей среде или привести к значительным финансовым убыткам и сбоям в функционировании органов государственной власти[40]. Под руководством ABW в 2015 году разработана и Доктрину кибербезопасности Польши, которая оперирует ключевыми понятиями теории безопасности типа «угроз» и «вызовов», «рисков» и тому

подобное. В 2015 году в Польше начата работа над Доктриной информационной безопасности.

Среди угроз информационной безопасности в Доктрине названы следующие:

-эскалация напряженности в международных отношениях;

-дискредитация польской международной политики и формирование негативного имиджа страны на международной арене, в том числе и среди союзников по НАТО и ЕС;

-формирование образа Польши как страны ксенофобов и антисемитов;

-провоцирование польско-литовского конфликта на фоне польского меньшинства в Литве;

-подстрекательство польско-украинского конфликта на сложном историческом фоне с возможным применением террористических покушений, которые якобы могли бы осуществить украинцы против поляков или наоборот.

Доктрина информационной безопасности Польши рассматривается как исполнительный документ к Стратегии национальной безопасности[46]. Важным аспектом, который уместно и развивать является привлечение в Польше к борьбе с информационными угрозами гражданское общество. В частности, успешным примером такой деятельности является созданная в 2018 году неправительственная организация - Центр анализа пропаганды и дезинформации. Данный Центр занимается выявлением и противодействием российской пропаганде. Указанная фонд является первым такого рода учреждением в Польше, деятельность которой направлена на анализ и поиск системного подхода к идентификации и противодействия российской дезинформации в польском информационном пространстве.

Кроме научно-исследовательской и аналитической работы, Центр будет сотрудничать с другими субъектами, чтобы заложить фундамент понимания в польском обществе угроз, поскольку информационная и психологическая война проникает в различные сферы жизнедеятельности общества и государства[133]. Другой особенностью правового обеспечения информационной безопасности в

Польшу и ряде других стран Восточной Европы, является непосредственное влияние на политику государства в информационной сфере вступление в НАТО. Это побудило страны к приведению в соответствие к стандартам НАТО национальное информационное законодательство. Примером этого можно назвать принятый в январе 1999 года закон «О защите конфиденциальной информации», принятие которого было одним из условий вступления Польши в НАТО[191].

Другим примером такого процесса является принятый в 1995 году закон Венгрии о государственные и официальные секреты [143]. В целом же венгерская политика в сфере обеспечения информационной безопасности настроена преимущественно на ограничение. Так, закон о средствах массовой информации (2010) вызвал критику со стороны мировых медиа и ЕС - Венгрию обвинили во введении тотального контроля за СМИ, включая интернет, в ликвидации свободы слова, даже в стремлении установить тоталитарный режим. Европейский парламент принял резолюцию[143] (впервые в отношении страны – члена ЕС) с осуждением того, как венгерское правительство относится к демократии, свободы слова, прав человека. Впоследствии парламент Венгрии внес косметические поправки к этому закону, которые впрочем не коснулись ключевых вопросов (структуры управления венгерскими СМИ), но были восприняты ЕС положительно [140].

Венгрия стала первой из постсоциалистических стран, которая приняла «Закон о защите информации о лице и доступ к информации, представляющей общественный интерес» (1992), которым, в частности, введен институт Парламентского комиссара по защите информации и свободы информации[129].

Согласно этому закону лицо, чьи персональные данные обрабатываются, необходимо полностью проинформировать о цели этих действий. Допускается сбор исключительно тех данных, которые необходимы для достижения указанной цели, а храниться они могут только в течение срока, пока цель не

будет достигнута. Каждому предоставляется право получать доступ к своей персональной информации и в случае необходимости потребовать ее исправления или уничтожения. Особая защита предусмотрена для так называемых «чувствительных» (sensitive) данных, касающихся «расового происхождения, национальности и этнического статуса, политических мнений или партийной принадлежности, религиозных или иных убеждений» или « сведений о болезнях, сексуальной жизни или судимости». Кроме того, правовую основу обеспечения информационной безопасности в части защиты персональных данных в Венгрии составляют законы «О праве на информационное самоопределение и свободу информации» (2011) и «Об обработке и защите медицинской информации и связанных с ней персональных данных» (1997). По любым вопросам, связанным с защитой персональных данных, лицо может обратиться к Национальному бюро по защите данных и свободы информации[47].

Правовое обеспечение информационной безопасности Венгрии, в т. ч. кибербезопасности, воплощено в законе «Об электронной информационную безопасность государственных и муниципальных органов» (2013) [48]и п. 31 Стратегии национальной безопасности Венгрии, утвержденной в 2012 году[49].

Стратегия национальной безопасности, в частности, предусматривает, что государство должно быть готово управлять рисками и угрозами, связанными с национальной безопасностью, обороной, борьбой против преступности, а также предотвращать нештатных ситуаций в киберпространстве, гарантировать адекватный уровень кибербезопасности и выполнять другие задачи, связанные с обеспечением кибербезопасности. При этом основной задачей признается систематическое определение приоритетов в сфере потенциальных угроз и рисков в киберпространстве, а также повышение информированности общества о них. Соответствующие положения получили дальнейшее развитие в Национальной стратегии кибербезопасности Венгрии, утвержденной 2013 года [50].

Довольно интересные есть опыт правового обеспечения информационной безопасности государства в Хорватии. В этой стране еще с 2007 года действует Акт об информационной безопасности [51]. Этим законодательным актом определены понятия информационной безопасности, ее элементы, меры обеспечения и стандарты, а также функциональные компетентности органов для принятия и реализации решений в сфере противодействия угрозам и обеспечении информационной безопасности государства, а также надзора за соблюдением соответствующих стандартов. В 2015 году в Хорватии принято национальную стратегию кибербезопасности [52], которая базируется на следующих основных принципах:

• всесторонность подхода к кибербезопасности, что охватывает киберпространство, инфраструктуру и пользователей в соответствии с хорватской юрисдикции (гражданство, регистрация, домен, адрес);

• интеграция мероприятий в различных сферах обеспечения кибербезопасности;

• проактивность благодаря постоянному корректировке мероприятий и периодическому уточнению их стратегических границ;

• укрепление устойчивости, надежности и управляемости путем применения универсальных критериев конфиденциальности, целостности и доступности определенных групп информации и социальных ценностей;

• защита прав и свобод человека в киберпространстве, прежде всего, конфиденциальности и собственности;

• постоянное совершенствование правовой базы;

• субсидиарность при распределении полномочий; соответствие расходов на обеспечение кибербезопасности степени риска и тому подобное.

Стратегия киберзащиты является частью стратегии обороны, что является сферой ответственности Министерства обороны Хорватии. Кибертерроризм, киберпреступность и некоторые другие кибернетические аспекты национальной безопасности рассматриваются также компетентными органами в системе безопасности и разведки, как нуждающиеся в специальном подходе.

Следует отметить, что обеспечение информационной безопасности, в том числе путем активных информационных операций, в конце прошлого века стало важным компонентом борьбы Хорватии за свои временно оккупированные территории, где более четырех лет существовала сепаратистская «Республика Сербская краина». При этом, по оценкам экспертов, если в милитарном смысле борьба за возвращение указанных территорий закончилась в августе 1995 года во время операции «Буря», в дипломатическом – в начале 1998-го, одновременно с мирной реинтеграцией хорватского Подунавья, то в информационном смысле война закончилась лишь через 15 лет после окончания боевых действий.

По результатам проведенных научных исследований, сейчас первоочередного внимания требуют такие ключевые угрозы национальной и международной безопасности в информационной сфере:

– глобальные изменения и трансформации в информационной сфере формируют новейшие вызовы и угрозы, которые представляют реальную угрозу безопасности человечества и международного правопорядка;

– в информационном пространстве наблюдается тенденция к распространению информационной агрессии и насилия, манипуляции сознанием человека и общества, периодически проводятся информационно-психологические операции;

– большинство стран мира столкнулась с проблемами кибершпионажа, кибертерроризма, киберпреступности и кибератаками на объекты критической инфраструктуры;

– последствия использования современного информационного оружия могут приводить к реальной потере государственного суверенитета и территориальной целостности стран мира.

Кроме проведенного анализа, важным представляется и опыт других стран Европейского пространства, которые проходят аналогичный путь евроинтеграции.

Поэтому исследования, оценка и имплементация положительных достижений этих стран имеют большое значение при построении системы обеспечения информационной безопасности в РФ, поскольку события последних лет в нашей стране показали, что мы пока что не готовы должным образом вести информационные войны, а политика в сфере обеспечения информационной безопасности и информационная политика в целом требуют совершенствования.

Интересные есть опыт Румынии и Болгарии как членов НАТО и Европейского Союза. В первую очередь потому, что в этих странах уже апробированы и действуют стандарты ЕС и НАТО по информационной политики и правового обеспечения информационной безопасности. В частности, это стандарты НАТО по защите информации, изложенные в Документе СМ (2002)49 «Безопасность в организации Североатлантического договора (НАТО)»[10], официальная политика НАТО в сфере киберзащиты[24], стратегическая концепция кибербезопасности, сформулированная по результатам Лиссабонского[25] и уточнена по результатам Варшавского саммитов, и др.

Как члены ЕС эти страны воплощают также в национальной политике обеспечения информационной безопасности стандарты ЕС, в том числе согласно «Европейским критериям безопасности информационных технологий» (1991) [11], «Единым критериям безопасности информационных технологий» (1996) [27], документами «Сетевая и информационная безопасность: европейский политический подход» (2001) [30] и «На пути к общей политики в сфере борьбы с киберпреступностью» (2007) [33] и др.

Анализ упомянутых международных документов позволяет выделить приоритетные направлениями обеспечения информационной безопасности в этих странах:

•повышение осведомленности пользователей о возможных угрозах при пользовании коммуникационными сетями;

•создание европейской системы предупреждения и информирования о новых угрозах;

•обеспечение технологической поддержки;

•поддержка рыночно ориентированной стандартизации и сертификации;

•правовое обеспечение, приоритетами которого является защита персональных данных, регламентация телекоммуникационных услуг и противодействие киберпреступности;

• укрепление информационной безопасности на государственном уровне путем внедрения эффективных и совместимых средств обеспечения информационной безопасности и поощрения использования государствами-членами электронных подписей при оказании государственных онлайн услуг и т. п.;

• развитие международного сотрудничества по вопросам информационной безопасности.

Основными вызовами информационной безопасности Румынии и Болгарии как членов ЕС являются:

• некоординированные национальные подходы к безопасности информационных инфраструктур, снижает эффективность национальных мер;

•отсутствие на европейском уровне партнерства между государственным и частным секторами;

• ограниченные возможности раннего предупреждения и реагирования на инциденты безопасности, обусловленные неравномерностью развития систем мониторинга и оповещения об инцидентах в странах-членах, неразвитостью межгосударственного сотрудничества и обмена информацией по этим проблемам;

• отсутствие международного консенсуса по приоритетам в реализации политики защиты критической информационной инфраструктуры [34].

Несмотря на указанные приоритеты важно значение на уровне законодательства предоставляется защите персональных данных. В Директиве 95/46/ЕС «О защите физических лиц в контексте обработки персональных

данных и свободного обращения таких данных» декларируется стремление к свободному перемещению информации между странами-членами ЕС и предоставляются гарантии защиты основных прав граждан, к которым относится право на неприкосновенность личных данных и их защиту от третьих лиц[194].

Важным новшеством является также введение более строгого наказания за несвоевременное сообщение информации об утечке данных. Компаниям, нарушившим положения новой директивы и не доложили о факте утечки или взлома в течение 72 часов с момента выявления инцидента, грозит штраф до 4% годового дохода или до 20 млн. евро[130].

Кроме того, соответствующая Директива предусматривает необходимость получения согласия пользователей на обработку их персональных данных, причем на обработку данных с различными целями нужны отдельные согласия. Согласие должно быть свободным, сознательным и конкретным, а также может быть отозвана в любой момент. Согласие не будет считаться свободным, если пользователь вынужден ее дать, чтобы получить доступ к сайту, приложению или приложению. Исключением являются случаи, когда персональные данные пользователя нужны для выполнения соглашения. В том случае, когда персональные данные собираются и обрабатываются для маркетинговых целей, пользователь должен иметь возможность не соглашаться со сбором и обработкой его данных. Компании, работающие с персональными данными, должны также вести учет операций с персональными данными (тип данных и цель их обработки), минимизировать использование персональных данных в соответствии с принципом data protection by design, а также проводить внутренний аудит[164].

В Румынии тоже достаточно строгий подход к данному вопросу. Так, в Румынии в настоящее время идет активный процесс развития системы кибернетической безопасности государства как на законодательном, так и на организационном уровнях. При этом ключевая роль в обеспечении кибербезопасности Румынии отводится ее специальном

контрразведывательному органу – Румынской службе информации, в структуре которой создан национальный центр кибербезопасности.

Главной функцией этого центра является сочетание систем технической защиты с возможностями спецслужбы с целью получения информации, необходимой для предупреждения, пресечения и ликвидации последствий кибератак на информационно-телекомуникационные системы объектов критической инфраструктуры государства[192].

Законопроект «О кибербезопасности», который в декабре 2014 года был одобрен сенатом Румынии, предусматривает также создание Национальной системы кибернетической безопасности Румынии, техническую координацию которой возложена на Румынскую службу информации как главного субъекта обеспечения кибербезопасности государства[193].

Особое внимание Национальная стратегия обеспечения кибербезопасности Румынии (2013) уделяет развитию национальных возможностей по управлению рисками в сфере кибернетической безопасности[55].

Пункт 4.7.3 Стратегии предусматривает создание механизмов и технических ресурсов для постоянного мониторинга возможных угроз кибербезопасности с точки зрения масштабов, источников и природы (кибер-, гибридные), тенденций в геополитическом контексте и анализа национальной картины кибербезопасности, а также развития способности применять адекватные формы противодействия, в том числе поддерживать создание источников контр-информационных воздействий[53].

Систему противодействия киберпреступности Молдовы, несмотря на критику учеными страны политики государства по обеспечению информационной безопасности в[165], можно считать относительно надежной. Так, еще в 2009 году парламент этой страны ратифицировал Конвенцию Совета Европы о киберпреступности. Кроме того, в марте 2012 года Молдова подписала Второй дополнительный Протокол к Европейской Конвенции о взаимной помощи по уголовным делам. Принят также закон «О

предупреждении и борьбе с преступностью в сфере компьютерной информации» (январь 2010 года)[54].

Согласно этому закону Генеральная прокуратура Молдовы наделена полномочиями координировать и осуществлять уголовное преследование лиц, совершивших киберпреступления. Целью закона является совершенствование регламентации правоотношений по следующим направлениям: предотвращение и борьба с киберпреступностью, содействие провайдерам и пользователям информационных систем, сотрудничество государственных служб с неправительственными организациями и другими представителями гражданского общества, а также международное сотрудничество с организациями и странами, которые имеют опыт в соответствующих вопросах.

Генеральная прокуратура с целью содействия расследованиям открыла Центр расследования киберпреступлений, один из отделов которого уполномочен реагировать на случаи угроз безопасности в правительственных структурах, бизнесе и общественном секторе. Кроме указанного в Молдове осуществлен ряд важных мер на пути укрепления национальной информационной безопасности. В частности, в результате ратификации Факультативного протокола к Конвенции ООН о правах ребенка, касающийся торговли детьми, детской проституции и порнографии, Конвенции Совета Европы о киберпреступности и Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия [56]Молдова стала активным участником процесса применения общей уголовной политики в сфере борьбы с информационной преступностью, в том числе преступлениями, связанными с онлайн-эксплуатацией детей.

Другим важным мероприятием на национальном уровне стало принятие закона «Об электронной подписи и электронном документе» (29 мая 2014 года), разработанного с целью повышения уровня безопасности электронных подписей и приведение в соответствие с международными стандартами и рекомендациями относительно инфраструктуры открытых ключей.

В целом следует заметить, что в Молдове начат процесс приведения действующего законодательства в соответствие с положениями Директивы 2006/24/ЕС от 15 марта 2006 года о хранения информации, созданной или обработанной при предоставлении услуг связи общего пользования или сетей связи общего пользования, и внесения изменений в директивы ЕС о защите персональных данных 2002/58/ЕС [4] и 2008/114/ЕС от 8 декабря 2008 года об идентификации и назначения европейских критических инфраструктур и оценку необходимости улучшения их защиты [57]и др.

В Молдове в 2013 году принята Национальная стратегия развития информационного общества «Moldova digitală 2020» («Цифровая Молдова 2020») и План действий по ее внедрению, разработанный Министерством информационных технологий и связи[157].

В Стратегии впервые рассматривается проблема создания условий для повышения степени безопасности и доверия к киберпространству, а ключевые действия по созданию этих условий составляют отдельную главу вышеупомянутого Плана действий. Стратегия определяет, что использование новых технологий порождает много возможностей для развития, но и многочисленные риски и уязвимости, требующие повышенного внимания государства и заинтересованных участников. Эти риски характеризуются асимметрией, выраженной динамикой и глобальным характером, что затрудняет их выявление и противодействие с помощью мер, пропорциональных эффекту их материализации.

Таким образом, предупреждения кибератак и борьба с ними, в том числе с преступностью в этой сфере, является одним из приоритетов международных организаций, а бурный рост числа кибератак на мировом уровне (на 600% с 2005 года) указывает на настоятельную необходимость принятия мер по страхованию информационной инфраструктуры Республики Молдова от возможных рисков, связанных с незаконной деятельностью в этой сфере. Важность этой проблемы была подчеркнута в Концепции национальной безопасности и Стратегии национальной безопасности Республики Молдова,

где определены цели системы обеспечения национальной безопасности и угрозы в информационной сфере.

По мнению экспертов, последние инициативы по регламентации информационного пространства содержат целый ряд серьезных пробелов, которые могут привести к злоупотреблениям. В частности, Концепцию информационной безопасности целесообразно согласовать с новой Стратегией национальной безопасности, однако последний проект Стратегии национальной безопасности в июне 2017 года был отозван из парламента президентом, а новый проект до сих пор не разработан.

Кроме того, проект Концепции предусматривает строгий контроль Интернета со стороны некоторых государственных учреждений, в частности Службы информации и безопасности Республики Молдова, которые смогут вмешиваться в деятельность провайдеров, а также контролировать информационное пространство, включая социальные сети [158].

Интересен опыт Белоруссии, где надзор за информационным пространством и система ограничений являются сейчас ключевыми элементами государственной информационной политики. С 2010 до 2015 года в стране действовало постановление Оперативно-аналитического центра при президенте и Министерства связи и информатизации Республики Беларусь от 29.06.2010 №4/11 «Об утверждении Положения о порядке ограничения доступа пользователей интернет-услуг к информации, запрещенной к распространению в соответствии законодательных актов». Постановление приписывала провайдерам фильтровать интернет-контент согласно двух черных списков url-адресов, один из которых находился в публичном доступе, а другой был доступен только провайдерам (закрытый список содержал примерно 80 url-адресов, доступ к которым государственных, культурных и правительственных учреждений ограничивался, и содержал популярные оппозиционные сайты вроде Charter97.org и Belaruspartisan.org)[128].

В настоящее время соответствующие ограничения реализуются в соответствии с указом президента Беларуси от 1 февраля 2010 года № 60 «О

мерах по совершенствованию использования национального сегмента сети Интернет», декрета президента от 28 декабря 2014 года «О неотложных мерах по противодействию незаконному обороту наркотиков» и закона Республики Беларусь от 17 июля 2008 года «О средствах массовой информации»[39].

В марте 2010 года от белорусских провайдеров потребовали более плотного сотрудничества с государственными системами наблюдения (СОРМ), которые осуществляют полный онлайн-наблюдение по всей стране, что регламентируется значительным количеством нормативно-правовых актов. Как и в России и соседних странах, СОРМ Беларуси с целью борьбы с преступностью дает исполнительным органам и органам национальной безопасности возможность перехватывать сообщения из любых коммуникационных каналов. Провайдеры интернет-услуг и операторы связи обязаны устанавливать соответствующее оборудование и предоставлять государственным органам круглосуточный доступ к нему.

Согласно указу «О мерах по совершенствованию использования национального сегмента сети Интернет» № 60 [37]провайдеры должны вести учет Ip-адресов, а государство может истребовать информацию относительно интернет-деятельности любого гражданина. С 2007 года в интернет-кафе выдвигается требование сохранять историю интернет-активности пользователей в течение года и информировать исполнительные органы о подозрительных действиях [35].

СОРМ работает в основном в соответствии с законами «Об оперативно-розыскной деятельности», «Об органах государственной безопасности Республики Беларусь» [36] и указа № 129 «Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность» [37].

В Беларуси нет специальных законов, посвященных противодействию киберпреступности, но некоторые аспекты регулируются Уголовным кодексом и законами, касающихся регламентации деятельности глобальной информационной сети Интернет. Беларусь также подавала заявку на

присоединение к Конвенции о киберпреступности, принятой в Будапеште в 2012 году[169], что и определило необходимость придерживаться соответствующих международных стандартов. Такой шаг Беларуси стал весьма неожиданным, особенно в контексте их тесных связей с Россией, ведь Китай и РФ выступили против конвенции и высказались в защиту альтернативной концепции борьбы с киберпреступностью, по которой государство получает значительно больше полномочий, чем это предполагается Будапештской конвенцией.

Расследованием компьютерных преступлений в Беларуси занимается специальное управление Министерства внутренних дел, которое координирует работу с другими исполнительными органами внутри страны и аналогичными международными организациями в США, Евросоюзе, странах СНГ и в других государствах. В обществе высказываются неединичные подозрения, что это управление занимается преимущественно преследованием уголовных правонарушителей, а никак не разработкой законодательства по вопросам кибербезопасности, а также участвует в преследовании и онлайн-отслеживании политических активистов.

Что касается участия Республики Беларусь в обеспечении кибербезопасности на региональном уровне, то следует отметить, что Совет глав государств Содружества Независимых Государств в 2013 году приняла Концепцию сотрудничества государств-членов СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий[3]. Согласно этому документу страны-члены СНГ обмениваются рабочей, статистической и методологической информацией и ведут единую базу данных киберпреступников. На основании этой Концепции с 2015 года осуществляется разработка программы сотрудничества между странами СНГ в борьбе с киберпреступностью, которая подлежит утверждению Советом министров стран СНГ.

Таким образом, в условиях развития технологий обеспечение информационной безопасности выступает одной из важнейших гарантией прав

человека. В основе таких гарантий лежит соблюдение принципов конфиденциальности, целостности и доступности информации и информационных систем. Для обеспечения информационной безопасности личности осуществляется выработка специальных правовых принципов защиты права на неприкосновенность частной жизни, а также дополнительных механизмов его защиты, связанных с установлением специфических требований в сфере сбора и обработки личной информации. При обеспечении национальной безопасности и информационной безопасности государства как одной из ее составляющих важнейшей гарантий прав человека выступает соблюдение принципа соразмерности при их ограничении. Реализация данных принципов и механизмов защиты прав человека при обеспечении информационной безопасности может принимать различные формы, которые зависят от правовых традиций и политического режима государства.

3.3. СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

Между государством и гражданским обществом возникает коллизия, связанная с возможностью реализацией права на доступ к информации и формируемой ограничениями вокруг нее. В принятых государством законах усматриваются нарушения ряда статей Конституции РФ, а именно:

1) закон ограничивает доступ граждан к незапрещенной информации, что является прямым нарушением конституционного права на получение и распространение информации (ч. 4 ст. 29 Конституции РФ);

2) закон, позволяющий блокировать IP-адрес, на котором кроме страниц или сайтов с запрещенной информацией существуют другие легальные сетевые ресурсы, фактически вводит коллективную ответственность за правонарушения (ч. 2 ст. 54 Конституции РФ);

3) права и свободы гражданина могут быть ограничены федеральным законом, но только в той мере, в какой это необходимо и если это преследует определенные цели. Данные законы превышают допустимые нормы и наносят

больший вред, чем правонарушения, с которыми они должны бороться (ч. 3 ст. 55 Конституции РФ).

Блокировка интернет-ресурсов по IP-адресам и цепная реакция, которая была отмечена выше, приводит к ограничению доступа к информации, которая соответствует законам и разрешена на территории Российской Федерации, тем самым умаляя права и свободы граждан на доступ к информации. Отсутствие четко прописанного регламента отсеивания информации, которая является запрещенной согласно законам, приводит к злоупотреблению указанным Конституцией допустимым ограничением. До тех пор, пока не будет четкого представления, что же и в какой мере является запрещенной информацией, коллизия будет существовать.

Данному конфликту между государственной безопасностью и информационной открытостью не место в современном демократическом обществе. Государственная безопасность ни в коем роде не может перекрывать информационную открытость, так как последняя является ведущим принципом социальной организации.

Особый интерес, на наш взгляд, представляет закрепленный в Доктрине информационной безопасности Российской Федерации[50] принцип деятельности органов государственной власти, который звучит как «соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в т.ч. в информационной сфере», в то время как предыдущая Доктрина базировалась на принципе свободного информационного обмена. В этой связи актуальным представляется вопрос, являются ли обоснованными ограничения свободного информационного обмена в новой Доктрине.

Рассуждая на поставленный вопрос, представляется убедительной позиция А.В. Туликова, который отмечает, что «неограниченный приоритет как информационной безопасности, так и информационной свободы вступает в противоречие с правовыми ценностями и принципами правового государства и

автономией личности. Несмотря на то, что между ними существует конфликт, они взаимосвязаны – свобода может быть выражена через безопасность, которая определяет ее пределы. Каждая из этих правовых ценностей выступает опорой для другой и выражается через нее. Это означает, что в системе правовых ценностей они находятся на одном уровне и соотношение между ними является равновесным»[172].

Объясняется это, на наш взгляд, тем, что абсолютная, безграничная свобода не может гарантировать безопасность, а государство с тотальным контролем и ограничениями нельзя назвать свободным. Между свободой и безопасностью необходимо поддерживать баланс, предполагающий разумные правовые ограничения с целью обеспечения информационной безопасности в целом и права личности на информационную безопасность в частности.

Закрепление данного принципа в новой Доктрине является адекватным ответом на вызовы современного информационного общества, где все чаще и чаще информационные технологии используются в противоправной деятельности. А реализация указанного принципа представляется одним из эффективных способов обеспечения права личности на информационную безопасность.

Анализ последних нововведений в сфере обеспечения права личности на информационную безопасность позволяет обнаружить тенденцию к использованию указанного в Доктрине принципа в иных нормативных правовых актах и активную реакцию на него со стороны общественности и средств массовой информации. Широкое обсуждение в обществе получил так называемый в средствах массовой информации «Пакет Яровой», под которым понимаются изменения, внесенные в ряд федеральных законов, имеющие антитеррористическую и антиэкстремистскую направленность, а также нацеленные на борьбу с противоправным контентом.

Особого интереса в контексте проводимого исследования заслуживают нормы, направленные на противодействие распространению противоправного контента. Так, с 1 июля 2018 г. на оператора связи возлагается обязанность по

хранению сообщений электросвязи в нулевом объеме, а с 1 октября 2018 г. – по хранению в полном объеме сообщений электросвязи в течение 30 суток. При этом по требованию уполномоченных государственных органов, осуществляющих оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в установленных законодательством случаях операторы связи обязаны предоставить вышеуказанные данные[106].

Данные поправки вызвали множество споров в обществе, которые были аргументированы тем, что указанные изменения нарушают неприкосновенность частной жизни, могут стать причиной утечки конфиденциальной информации и требуют значительных материальных затрат от организаторов распространения информации, что, в свою очередь, отразится и на пользователях. Подобные мнения высказывались и в научной литературе. Так, А.В. Шигуров в своей работе дает критический анализ новых положений и отмечает, что внесение рассматриваемых изменений было ошибочным шагом законодателя, ограничивающим конституционные права человека несоразмерно тем целям, которые он декларирует, и ожидаемым положительным последствиям[181].

Е.В. Злотникова отмечает, что «совершенствование антитеррористических мер приводит к систематическому ограничению демократических прав и свобод граждан, за которые они боролись на протяжении длительного периода истории»[139].

Мы, в свою очередь, полагаем, что рассмотренные поправки не нарушают права и свободы человека и гражданина ввиду того, что вышеуказанные данные могут быть запрошены уполномоченными органами в предусмотренных законом случаях, в связи с нарушением гражданином закона. При иных обстоятельствах переписка граждан либо аудио-, видео- или иные сообщения никаким образом обнаружены быть не могут. Как и прежде, операторы сети будут обязаны шифровать данные, а уполномоченные органы смогут получить ключи шифрования только по судебному запросу. При этом Пленум Верховного Суда Российской Федерации разъясняет, что факты доступа к

вышеуказанным данным без судебного разрешения либо без согласия лица, которому эти данные принадлежат, будут являться нарушением тайны переписки и телефонных переговоров[110].

Вместе с тем считаем, что принятые «Пакетом Яровой» поправки в законодательство имеют позитивное значение в том случае, когда появится необходимость доступа к личной переписке в целях предъявления ее в качестве доказательства в суде при необходимости защиты права личности на информационную безопасность. Это может быть актуально, например, при противодействии кибербуллингу, который получает все большее распространение на территории Российской Федерации. Кроме «Пакета Яровой», в сфере обеспечения права личности на информационную безопасность общественный резонанс вызвало также постановление Правительства Российской Федерации, направленное на урегулирование работы мессенджеров[111].

Согласно данному постановлению, на организатора обмена мгновенными сообщениями (мессенджера) возлагается обязанность по идентификации пользователей по номеру телефона. Иными словами, пользоваться мессенджером сможет только тот абонент, на которого оформлена сим-карта. Мобильные операторы на основании запроса от мессенджера будут обязаны предоставлять информацию об абоненте. Если в течение 20 минут с момента получения запроса оператор не предоставит данную информацию о пользователе либо уведомит о том, что в базе данных о нем отсутствует информация, доступ пользователя к мессенджеру будет прекращен и впоследствии заблокирован. Вместе с тем стоит отметить, что Министерством цифрового развития, связи и массовых коммуникаций выработаны строгие требования по отношению к операторам персональных данных, занимающихся их сбором и обработкой, за нарушение которых предусмотрена административная ответственность в виде штрафа. Представляется, что рассмотренные меры по идентификации пользователей мессенджеров станут основой для создания безопасной коммуникационной среды, обеспечивающей

воз-можности личности по реализации права свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Пленум Верховного Суда Российской Федерации также не остался в стороне при обсуждении «дел о лайках и репостах». 20 сентября 2018 г. было принято постановление, содержащее рекомендации для судей при рассмотрении подобных дел.

В постановлении говорится о том, что «гарантированные Конституцией и международно-правовыми актами свобода мысли и слова <…> могут быть ограничены только в исключительных случаях». Пленум призывает судей при рассмотрении дел об «экстремизме в социальных сетях» изучать данные о личности обвиняемого на предмет приверженности радикальной идеологии, участия в экстремистских объединениях, привлечения ранее к административной или уголовной ответственности. При этом необходимо также учитывать факт личного создания либо заимствования лицом соответствующих аудио-, видеофайлов, текста или изображения, содержание всей страницы данного лица, сведения о деятельности такого лица до и после размещения информации, в т.ч. о совершении действий, направленных на увеличение количества просмотров и пользовательской аудитории[123].

Такое внимание со стороны государственных органов к данной проблеме обусловлено необходимостью преодоления формализма и установления законодательных пределов ограничения свободы слова при привлечении к ответственности по делам об экстремизме. Свобода мысли и слова, свобода выражения мнений и убеждений являются важным аспектом обеспечения права личности на информационную безопасность. При этом, как уже отмечалось выше, указанные свободы не могут быть неограниченными и неприкосновенными, в отношении них должны действовать определенные ограничения, с одной стороны, защищающие личность от намеренного злоупотребления такой свободой и, с другой стороны, препятствующие

государству применять карательные меры за высказывания, противоречащие официальной точке зрения.

Подводя итог вышеизложенному, стоит согласиться с выводами А.К. Жаровой о том, что «в XXI веке информация выступает в качестве нового класса социальных ресурсов, существующих, с одной стороны, независимо от человека, но, с другой стороны, формирующихся самим человеком на протяжении истории развития общества. Обладание данным ресурсом, его защита и безопасность рассматриваются как необходимая составляющая государственного суверенитета»[138]. При этом право на свободу информационного обмена должно признаваться и гарантироваться государством.

Однако абсолютная свобода влечет за собой определенные, вполне обоснованные риски и угрозы праву личности на информационную безопасность, а также всей государственной безопасности в целом. Поэтому закрепленный в Доктрине информационной безопасности принцип «соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере» является вполне обоснованным и основан на части 3 статьи 55 Конституции Российской Федерации, которая определяет, что «права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, обеспечения обороны страны и безопасности государства».

По нашему мнению, регулирование интернета должно учитывать следующие моменты:

1) в решении вопроса о государственной безопасности, невозможно ограничиться только национальным законодательством, необходимо использовать и развивать международные акты, поскольку сама архитектура Сети трансгранична. Подобный информационный контроль возможен в

отношении информации, что является запрещенной во всех странах (пропаганда терроризма, наркотиков, детская порнография и тд.);

2) многообразие источников правового регулирования Интернета влечет необходимость создания информационного кодекса, способного разрешать противоречия и конкуренцию норм, публичноправовых и частноправовых, а также национальных и международных. Так как с развитием информационного общества количество антагонизмов и сложностей, с которыми сталкивается отраслевой законодатель, будет лишь возрастать, что, однако, не дает ему права отходить от базовых принципов правового регулирования общественных отношений. На данный момент ситуация осложняется возникновением большого массива несистематизированных нормативных правовых актов, регулирующих их;

3) целесообразно введение в Гражданский процессуальный кодекс РФ отдельной главы, посвященной рассмотрению дел о признании информации запрещенной к распространению. Решения о признании информации запрещенной к распространению в сети Интернет должны публиковаться;

4) необходимо создание единого классификатора полномочий федеральных органов исполнительной власти в сфере информационной безопасности. Так как важно обеспечить баланс эволюции правового регулирования и стабильности законодательства.

ЗАКЛЮЧЕНИЕ

Ограничения гражданских прав и безопасность государства непосредственно связаны друг с другом. Появление угрозы безопасности Российской Федерации запускает механизм, который оказывает давление на свободы гражданских прав в угоду эффективности защиты. Нынешнее состояние страны, социально-политическая поляризация российского общества и осложнение международных отношений порождает широкий перечень возможностей для возникновения внешних и внутренних угроз безопасности государства.

Тем не менее можно констатировать, что действующее законодательство по ограничению прав и свобод граждан и организаций в целях предотвращения вооруженных конфликтов фактически не сформировано и не позволяет в полной мере реализовать общие особенности их правовой природы, что обусловливает необходимость и возможность закрепления указанных особенностей в отдельных федеральных законах, определяющих применение ограничений прав и свобод граждан и организаций, исходя из характера угроз в сфере защиты основ конституционного строя, обеспечения обороны страны и безопасности государства.

Выделенные способы и средства ограничения прав и свобод в интересах обеспечения обороны страны и безопасности государства, основанные на принципах данного правового института, установленных конституционно и в международных правовых актах, применяемые в соответствии с требованиями и нормативно установленными основаниями, выступают системообразующим, связующим звеном между субъектами ограничений прав и свобод личности и организации в интересах обеспечения обороны страны и безопасности государства. Их использование будет способствовать обеспечению безопасности личности, что является условием безопасности общества и государства.

Правомерное ограничение в условиях возникновения чрезвычайных ситуаций устанавливают только уполномоченные на то субъекты, с соблюдением определенной процедуры, определенной нормативно-правовыми актами.

Следовательно, можно прийти к выводу, что ограничения − это расширение полномочий органов государственной власти, а также уменьшение объема прав и свобод и законных интересов физических и юридических лиц.

Вопрос об установлении ограничений прав и свобод человека в законодательстве имеет как теоретическое, так и практическое значение. Первое заключается в лучшей определенности природы ограничений прав и свобод человека при выяснении этого вопроса и определении действия механизма правового регулирования в отношении таких ограничений. Второе является важным для адекватного установления ограничений прав и свобод человека в национальном законодательстве.

При этом важно подчеркнуть, что нередко ограничения прав и свобод человека содержатся в нормах законодательства, но чтобы их выяснить, следует применять теоретико-правовые приемы, которые и позволяют их обнаружить. Более того, выявление таких ограничений с помощью существующих юридических приемов необходимо, поскольку произвольное установление ограничений прав человека в правовом государстве невозможно и противоречило бы конституционным принципам и нормам. Поэтому ограничение прав и свобод человека должны опираться на развитые правовые теории и теоретически обоснованные механизмы их установления, они являются исключительными и должны быть обоснованными при их установке.

Блокировка интернет-ресурсов по IP-адресам и цепная реакция, которая была озвучена выше, приводит к ограничению доступа к информации, которая соответствует законам и разрешена на территории Российской Федерации, тем самым умаляя права и свободы граждан на доступ к информации. Отсутствие четко прописанного регламента отсеивания информации, которая является запрещенной согласно законам, приводит к злоупотреблению указанным

Конституцией допустимым ограничением. До тех пор, пока не будет четкого представления, что же и в какой мере является запрещенной информацией, коллизия будет существовать.

Данному конфликту между государственной безопасностью и информационной открытостью не место в современном демократическом обществе. Государственная безопасность ни в коем роде не может перекрывать информационную открытость, так как последняя является ведущим принципом социальной организации.

По нашему мнению, регулирование интернета должно учитывать следующие моменты:

1) в решении вопроса о государственной безопасности, невозможно ограничиться только национальным законодательством, необходимо использовать и развивать международные акты, поскольку сама архитектура Сети трансгранична. Подобный информационный контроль возможен в отношении информации, что является запрещенной во всех странах (пропаганда терроризма, наркотиков, детская порнография и тд.);

2) многообразие источников правового регулирования Интернета влечет необходимость создания информационного кодекса, способного разрешать противоречия и конкуренцию норм, публичноправовых и частноправовых, а также национальных и международных. Так как с развитием информационного общества количество антагонизмов и сложностей, с которыми сталкивается отраслевой законодатель, будет лишь возрастать, что, однако, не дает ему права отходить от базовых принципов правового регулирования общественных отношений. На данный момент ситуация осложняется возникновением большого массива несистематизированных нормативных правовых актов, регулирующих их;

3) целесообразно введение в Гражданский процессуальный кодекс РФ отдельной главы, посвященной рассмотрению дел о признании информации запрещенной к распространению. Решения о признании информации запрещенной к распространению в сети Интернет должны публиковаться;

4) необходимо создание единого классификатора полномочий федеральных органов исполнительной власти в сфере информационной безопасности. Так как важно обеспечить баланс эволюции правового регулирования и стабильности законодательства.

Таким образом, в условиях развития технологий обеспечение информационной безопасности выступает одной из важнейших гарантией прав человека. В основе таких гарантий лежит соблюдение принципов конфиденциальности, целостности и доступности информации и информационных систем. Для обеспечения информационной безопасности личности осуществляется выработка специальных правовых принципов защиты права на неприкосновенность частной жизни, а также дополнительных механизмов его защиты, связанных с установлением специфических требований в сфере сбора и обработки личной информации. При обеспечении национальной безопасности и информационной безопасности государства как одной из ее составляющих важнейшей гарантий прав человека выступает соблюдение принципа соразмерности при их ограничении. Реализация данных принципов и механизмов защиты прав человека при обеспечении информационной безопасности может принимать различные формы, которые зависят от правовых традиций и политического режима государства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Международные акты

1.Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета. 1995. 5 апреля.

2.Конвенция о защите прав человека и основных свобод: Совет Европы, Конвенция, Международный документ от 04.11.1950.

3.Концепция сотрудничества государств-участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий (утверждена Решением Совета глав государств СНГ от 25 октября 2013 года): URL: http://www.e-cis.info/page.php?id=23808 (дата обращения: 02.12.2019).

4.Директива N 2008/114/ЕС Европейского парламента и Совета Европы от 08 грудня 2008 року «О европейских критических инфраструктурах и мерах по их защите». URL: http://docs.pravo.ru/document/view/32671965/. (дата обращения: 02.12.2019).

5.Директива 95/46/ЕС Европейского Парламента и Совета «О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных» от 24 октября 1995 года.

6.Директива 95/46/ЕС Европейского Парламента и Совета «О защите физических лиц при обработке персональных данных и о свободном перемещении таких данных» от 24 октября 1995 года.

7.О доступе к информации, находящейся в распоряжении государственных органов: Рекомендации Совета Европы № R (81)19. URL: http://medialaw.org.ua/library/rekomendatsiya-r-81-19-pro-dostup-doinformatsiyi-shho-znahodytsya-u-rozporyadzhenni-derzhavnyh-organiv (дата обращение: 02.12.2019).

8.General Assembly Resolution «The right to privacy in the digital age», A/RES/68/167: URL: http://www.ohchr.org/EN/Issues/ DigitalAge/Pages/DigitalAgeIndex.aspx (дата обращения: 02.12.2019)

9.Across Europe? Nations Mold Cyber Defenses. URL: http:// archive.defensenews.com/article/20130709/DEFREG01/307090008/AcrossEuropr-Nations-Mold-Cyber-Defenses (дата обращения: 02.12.2019).

10.Document C-V(2002)49: Security within tne North Atlantic Treaty Organization (NATO). URL: www.statewatch.org/ news/2006/sep/nato-sec-classifications.pdf (дата обращения: 02.12.2019).

11.Information Tecnhology Security Evaluation Criteria. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf (дата обращения: 02.12.2019).

12.Children's Online Privacy Protection Act (1998), Gramm-Leach-Bliley Act EU (1999)

13.Fair Credit Report Act EU of 1992

14.Health Insurance Portability and Accountability Act EU (HIPAA) (1996)

15.Electronic Communications Privacy Act EU (1986)

16.Family and Educational Privacy Act EU (1974)

17. Video Privacy Protection Act EU (1988)

18. Telephone Customers Protection Act EU (1994)

19.Drivers Privacy Protection Act EU (1994)

20.Privacy Act EU (1974)

21.Communication of the European Commission, Strategy for the Effective Implementation of the Charter of Fundamental Rights by the European Union, COM (2010) 573/4, Brussels, 19.10.2010 // URL: http://ec.europa.eu/justice/news/intro/doc/com_2010_573_en.pdf (дата обращения: 31.10.2019)

22.General Data Protection Regulation (GDPR); European Parliament Legislative Resolution of March 12, 2014 on the Proposal for a Regulation of the

European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) // URL: http://www.europarl. europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN (дата обращения: 31.10.2019).

23.Document C-V(2002)49: Security within tne North Atlantic Treaty Organization (NATO). URL: www.statewatch.org/ news/2006/sep/nato-secclassifications.pdf (дата обращения: 02.12.2019)

24.NATO Bucharest Summit Declaration, 3 April 2008: [Online tool]. – Available at: http://www.nato.int/docu/pr/2008/p08-049e.html (дата обращения: 02.12.2019).

25.NATO Lisbon Summit Declaration, 20 Nowember 2010. URL: http://www.nato.int/docu/pr/2010/p10-049e.html (дата обращения: 02.12.2019).

26.NATO Warsaw Summit Communiqué, 9 July 2016 URL: http://www.nato.int/cps/en/natohq/official_texts_133169.htm (дата обращения: 02.12.2019).

27.Common Criteria for Information Technology Security Evaluation. URL:https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf (дата обращ: 02.12.2019).

28.Safer Internet Programme. URL: http://ec.europa.eu/ information_society/activities/sip/policy/programme/current_prog/index_en.htm (дата обращения: 02.12.2019).

29.Communication from the Commission: Towards a general policy on the fight against cyber crime. COM (2007). URL: 435 http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf (дата обращения: 02.12.2019).

30.Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298. URL: http://ec.europa.eu/information_society/eeurope/2002/ news_library/ pdf_files/netsec_en.pdf (дата обращения: 02.12.2019)

31.Common Criteria for Information Technology Security Evaluation. URL:https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf (дата обращения: 02.12.2019).

32.Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001). URL: http://ec.europa.eu/information_society/eeurope/2002/ news_library/ pdf_files/netsec_en.pdf (дата обращения: 02.12.2019).

33.Communication from the Commission: Towards a general policy on the fight against cyber crime. COM (2007). URL: http://eurlex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf. (дата обращения: 02.12.2019).

34.Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM (2009) URL: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ ciip/index_en.htm. (дата обращения: 02.12.2019).

Зарубежные нормативные правовые акты

35.Закон Республики Беларусь от 15 июля 2015 года No 307-З «Об оперативно-розыскной деятельности»: URL: http://kgb.by/ru/zakon289-3/ (дата обращения: 02.12.2019).

36.Закон Республики Беларусь от 10 июля 2012 года No 390-З «Об органах государственной безопасности Республики Беларусь»: URL: http://kgb.by/ru/zakon390-3/. (дата обращения: 02.12.2019).

37.Указ Президента Республики Беларусь от 01 февраля 2010 года No 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»: URL: http://pravo.by/ document/?guid=3871&p0=P31000060. (дата обращения: 02.12.2019).

38.Указ Президента Республики Беларусь от 03 марта 2010 года No 129 «Об утверждении Положения о порядке взаимодействия операторов

электросвязи с органами, осуществляющими оперативно-розыскную деятельность»: URL: http://oac.gov.by/ files/files/pravo/ukazi/Ukaz_129.htm. (дата обращения: 02.12.2019).

39.Постановление Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 года No 7/7 «О признании утратившим силу постановления Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 29 июня 2010 года No 4/11». URL: http://www.pravo.by/upload/docs/op/T21503058_1424811600.pdf (дата обращения: 02.12.2019).

40.Доктрина кибезбезопасности Польщи. URL: constitutions.ru/?p=11083 (дата обращения: 02.12.2019)

41.Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG. URL: http://www. gesetze - iminternet.de/s_g/BJNR086700994.html (дата обращения: 02.12.2019).

42.Teleservices Data Protection Act. URL: http://ourworld.compuserve.com/homepages/ckuner/multimd (дата обращения: 02.12.2019).

43.Federal Act Governing Access to Information held by the Federal Government (Freedom of Information Act). URL: http://www.gesetze-iminternet.de/ifg/BJNR272200005.html (дата обращения: 02.12.2019).

44.Stasi Files Act (Stasi-Unterlagengesetz, StUG). URL: http://germanlawarchive.iuscomp.org/?p=714 (дата обращения: 02.12.2019).

45.Act on the Federal Office for Information Security (BSI Act - BSIG). URL: https://www.bsi.bund.de/DE/DasBSI/Gesetz/ gesetz.html (дата обращ: 02.12.2019).

46.Biuro Bezpieczeństwa Narodowego. URL: en.bbn.gov.pl дата обращения: 02.12.2019).

47.Nemzeti Adatvédelmi és Információszabadság Hatóság (Hungarian National Authority for Data Protection and Freedom of Information): URL: http://www.naih.hu/uegyfelszolgalat,--kapcsolat.html (дата обращения: 02.12.2019).

48.Act on the Electronic Information Security of Central and Local Government Agencies): URL: http://njt.hu/cgi_bin/njt_doc.cgi?docid= 160206.240508 (дата обращения: 02.12.2019).

49.Hungary's National Security strategy (2012): URL: http://2010-2014.kormany.hu/download/4/32/b0000/National%20Security% 20Strategy.pdf (дата обращения: 02.12.2019).

50.National Cyber Security Strategy of Hungary (2013): URL: http://www.nbf.hu/anyagok/Government%20Decision%20No% 201139_2013%20on%20the%20National%20Cyber%20Security%20Strategy% 20of%20Hungary.docx (дата обращения: 02.12.2019).

51. Information security act of the Republic of Croatia (2007): URL: http://www.uvns.hr/UserDocsImages/en/dokumenti/info-security/Information-Security-Act.pdf (дата обращения: 02.12.2019).

52.The national cyber security strategy of the republic. URL: http://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20 National%20Cyber%20Security%20Strategy%20(2015).pdf (дата обращения: 02.12.2019).

53.National Cyber Security Strategy: Cyber Resilient Bulgaria 2020 (2016 URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf. (дата обращения: 02.12.2019).

54.Lege Nr. 20 din 03.02.2009 Privind prevenirea şi combaterea criminalităţii informatice. URL: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=333508&lang=1 (дата обращения: 02.12.2019).

55.Romania's Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013): [Online tool]. – Available at.

URL: https://www.cert.ro/vezi/document/strategia-de-securitate-cibernetica (дата обращения: 02.12.2019).

56.Lege Nr. 91 din 29.05.2014 Privind semnătura electronică şi documentul electronic. URL: http://lex.justice.md/viewdoc.php? action=view&view= doc&id=353612&lang=1 (дата обращения: 02.12.2019).

57.HOTĂRÎRE Nr. 811 din 29.10.2015 Cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020. URL: http://lex.justice.md/viewdoc.php?action=view&view=doc&id= 361818&lang=1. (дата обращения: 02.12.2019).

Нормативные правовые акты РФ

58.«Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ)//в «Собрание законодательства РФ», 04.08.2014, N 31, ст. 4398.

59.Федеральный конституционный закон от 30.01.2002 N 1-ФКЗ О военном положении»«// «Собрание законодательства РФ», 04.02.2002, N 5, ст. 375.

60.Федеральный конституционный закон от 30.05.2001 N 3-ФКЗ (ред. от 03.07.2016) «О чрезвычайном положении»//»Собрание законодательства РФ», 04.06.2001, N 23, ст. 2277.

61.Федеральный закон от 31.05.1996 N 61-ФЗ (ред. от 03.08.2018) «Об обороне»//»Собрание законодательства РФ», 03.06.1996, N 23, ст. 2750

62.Федеральный закон от 12.02.1998 N 28-ФЗ (ред. от 01.05.2019) «О гражданской обороне»//»Собрание законодательства РФ», 03.06.1996, N 23, ст. 2750

63.Федеральный закон от 21.12.1994 N 68-ФЗ (ред. от 03.08.2018) «О защите населения и территорий от чрезвычайных ситуаций природного и

техногенного характера»//»Собрание законодательства РФ», 26.12.1994, N 35, ст. 3648.

64.Федеральный закон от 21.12.1994 N 69-ФЗ (ред. от 26.07.2019) «О пожарной безопасности»//»Собрание законодательства РФ», 26.12.1994, N 35, ст. 3649

65.Федеральный закон от 10.12.1995 N 196-ФЗ (ред. от 27.12.2018) «О безопасности дорожного движения» (с изм. и доп., вступ. в силу с 01.11.2019)//»Собрание законодательства РФ», 11.12.1995, N 50, ст. 4873

66.Федеральный закон от 09.01.1996 N 3-ФЗ (ред. от 19.07.2011) «О радиационной безопасности населения»//»Собрание законодательства РФ», 15.01.1996, N 3, ст. 141

67.Федеральный закон от 21.07.1997 N 116-ФЗ (ред. от 29.07.2018) «О промышленной безопасности опасных производственных объектов»//»Собрание законодательства РФ», 28.07.1997, N 30, ст. 3588

68.Федеральный закон от 06.03.2006 N 35-ФЗ (ред. от 18.04.2018, с изм. от 29.03.2019) «О противодействии терроризму»//»Собрание законодательства РФ», 13.03.2006, N 11, ст. 1146.

69.Федеральный закон от 25.07.2002 N 114-ФЗ (ред. от 28.11.2018) «О противодействии экстремистской деятельности»//Собрание законодательства Российской Федерации от 29 июля 2002 г. N 30 ст. 3031

70.Федеральный закон от 07.08.2001 N 115-ФЗ (ред. от 02.08.2019) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»//» Собрание законодательства РФ», 13.08.2001, N 33 (часть I), ст. 3418.

71.Федеральный закон от 25.12.2008 N 273-ФЗ (ред. от 26.07.2019) «О противодействии коррупции»//» Собрание законодательства РФ», 29.12.2008, N 52 (ч. 1), ст. 6228

72.Федеральный закон «О государственной охране» (ст. 9); «О мобилизационной подготовке и мобилизации в Российской Федерации» (ст. 9, 10, 13)//СЗ РФ. 1996. N 22. Ст. 2594

73.Федеральный закон от 26.07.2006 N 135-ФЗ (ред. от 18.07.2019) «О защите конкуренции»//» Собрание законодательства РФ», 31.07.2006, N 31 (1 ч.), ст. 3434

74. Федеральный закон от 30.12.2012 N 302-ФЗ (ред. от 04.03.2013) «О внесении изменений в главы 1, 2, 3 и 4 части первой Гражданского кодекса Российской Федерации»//» Собрание законодательства РФ», 31.12.2012, N 53 (ч. 1), ст. 7627,

75.Федеральный закон от 17.08.1995 N 147-ФЗ (ред. от 29.07.2017) «О естественных монополиях»//» Собрание законодательства РФ», 21.08.1995, N 34, ст. 3426

76.Федеральный закон «О гражданской обороне» (ст. 4)//1997. N 9. Ст. 1014

77.Федеральный закон от 10.01.2002 N 7-ФЗ «Об охране окружающей среды»// «Российская газета», N 6, 12.01.2002.

78.Федеральный закон» О промышленной политике в Российской Федерации» (ст. 4, 12 - 14, 21)//1998. N 7. Ст. 799;

79.Федеральный закон «О стандартизации в Российской Федерации» (ст. 3) // 2015. N 1 (ч. I). Ст. 41; N 27. Ст. 3953.

80.Федеральный закон от 29.04.2008 N 57-ФЗ «О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства»// «Российская газета», N 96, 07.05.2008.

81.Федеральный закон от 28.12.2012 N 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» // «Российская газета», N 302, 29.12.2012.

82.Федеральный закон от 28.12.2010 N 390-ФЗО безопасности»// «Российская газета», N 295, 29.12.2010.

83.Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ //Собрание законодательства Российской Федерации от 3 января 2011 г. N 1 ст. 48

84. Федеральный закон от 28 июля 2012 г. N 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации» (с изменениями и дополнениями)//Собрание законодательства Российской Федерации от 30 июля 2012 г. N 31 ст. 4328

85.Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»/ «Российская газета», № 165, 29.07.2006

86.Федеральный закон от 24.07.1998 N 124-ФЗ (ред. от 16.10.2019) «Об основных гарантиях прав ребенка в Российской Федерации»//» Собрание законодательства РФ», 03.08.1998, N 31, ст. 3802,

87. Федеральный закон от 22 ноября 1995 г. N 171-ФЗ «О государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции»//Собрание законодательства Российской Федерации от 27 ноября 1995 г. N 48 ст. 4553

88. Федеральный закон «Об охране здоровья граждан от воздействия окружающего табачного дыма и последствий потребления табака» от 23.02.2013 N 15-ФЗ (последняя редакция)//Собрание законодательства Российской Федерации от 25 февраля 2013 г. N 8 ст. 721

89. Федеральный закон от 29 декабря 2006 г. N 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации»//Собрание законодательства Российской Федерации от 1 января 2007 г. N 1 (часть I) ст. 7

90.Закон РФ от 05.03.1992 N 2446-1 «О безопасности»//» Российская газета», N 103, 06.05.1992.

91.Указ Президента РФ от 31.12.2015 N 683» О Стратегии национальной безопасности Российской Федерации»//» Собрание законодательства РФ», 04.01.2016, N 1 (часть II), ст. 212.

92.Указ Президента РФ от 05.12.2016 N 646» Об утверждении Доктрины информационной безопасности Российской Федерации»// «Собрание законодательства РФ», 12.12.2016, N 50, ст. 7074.

93. Указ Президента РФ от 9 мая 2017 г. N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»//Собрание законодательства Российской Федерации от 15 мая 2017 г. N 20 ст. 2901

94.Указ Президента РФ от 30 января 2010 г. N 120 «Об утверждении Доктрины продовольственной безопасности Российской Федерации»//Собрание законодательства Российской Федерации от 1 февраля 2010 г. N 5 ст. 502

95.Указ Президента РФ «Об утверждении Концепции общественной безопасности в Российской Федерации (утв. Президентом РФ 14.11.2013)//Текст концепции официально опубликован не был

96.Указ Президента РФ «Об утверждении Концепции противодействия терроризму в Российской Федерации (утв. Президентом РФ 05.10.2009)//Российская газета от 20.10.2009. № 198

97.Указ Президента РФ от 9 июня 2010 г. N 690 «Об утверждении Стратегии государственной антинаркотической политики Российской Федерации до 2020 года»//Собрание законодательства Российской Федерации от 14 июня 2010 г. N 24 ст. 3015

98.Указ Президента РФ «Об утверждении Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период Российской Федерации до 2020 года/Текст концепции официально опубликован не был

99.Указ Президента РФ от 1 апреля 2016 г. N 147 «О Национальном плане противодействия коррупции на 2016 - 2017 годы»//Собрание законодательства Российской Федерации от 4 апреля 2016 г. N 14 ст. 1985

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

101.Указ Президента РФ от 13 мая 2017 г. N 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года»//Собрание законодательства Российской Федерации от 15 мая 2017 г. N 20 ст. 2902

102.Указ Президента РФ от 19 апреля 2017 г. N 176 «О Стратегии экологической безопасности Российской Федерации на период до 2025 года»//Собрание законодательства Российской Федерации от 24 апреля 2017 г. N 17 ст. 2546

103.Указ Президента от 25.12.2014 N Пр-2976 «Военная доктрина Российской Федерации»//»Российская газета», N 298, 30.12.2014

104. Указ Президента от 30.04.2012 «Основы государственной политики в области экологического развития Российской Федерации на период до 2030 года».

105.Указ Президента РФ от 06.05.2011 N 590 «Вопросы Совета Безопасности Российской Федерации»//» Собрание законодательства РФ», 09.05.2011, N 19, ст. 2721.

106.Указ Президента от 30.04.2012 Стратегия экономической безопасности Российской Федерации на период до 2030 года (// СПС «КонсультантПлюс».

107.Постановление Правительства РФ от 27 октября 2018 г. N 1279 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями»//Собрание законодательства Российской Федерации от 12 ноября 2018 г. N 46 ст. 7043

108.Постановление Правительства РФ от 26.02.2010 № 96 «Об антикоррупционной экспертизе нормативных правовых актов и проектов нормативных правовых актов» (вместе с «Правилами проведения антикоррупционной экспертизы нормативных правовых актов и проектов нормативных правовых актов», «Методикой проведения антикоррупционной экспертизы нормативных правовых актов и проектов нормативных правовых актов»)/ «Российская газета», № 46, 05.03.2010

109.Постановление Правительства РФ от 27.10.2018 № 1279Об утверждении правил идентификации пользователей информационно-телекоммуникационной сети Интернет организатором сервиса обмена мгновенными сообщениями:. Доступ из справ.-правовой системы «КонсультантПлюс».

110.Постановление Правительства РФ от 12.04.2018 № 445 Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи// Собрание законодательства РФ. 2018. № 17. Ст. 2489.

111.Распоряжение Правительства РФ от 02.12.2015 № 2471-р Об утверждении Концепции информационной безопасности детей// Собрание законодательства РФ. 2015. № 49. Ст. 7055.

112.Распоряжение Правительства РФ от 28.07.2017 N 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»// Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 03.08.2017,» Собрание законодательства РФ», 07.08.2017, N 32, ст. 5138.

113.Законопроект № 469143-7 «О внесении изменений в статью 15-1 Федерального закона «Об информации, информационных технологиях и о защите информации» в части установления дополнительных механизмов противодействия деятельности, направленной на побуждение детей к совершению противоправных действий, опасных для их жизни»

114.Закон Ставропольского края от 29 июля 2009 г. N 52-кз «О НЕКОТОРЫХ МЕРАХ ПО ЗАЩИТЕ ПРАВ И ЗАКОННЫХ ИНТЕРЕСОВ НЕСОВЕРШЕННОЛЕТНИХ»//» Сборник законов и других правовых актов Ставропольского края» N 21 (303), ст. 8415 от 15.09.2009

115.Закон Ставропольского края от 3 июля 2007 г. N 23-кз «О запрете деятельности по организации и проведению азартных игр на территории Ставропольского края»/Ставропольская правда от 04 июля 2007 года №156-157

116. Закон Ставропольского края от 1 марта 2005 г. N 4-кз «О некоторых вопросах государственной гражданской службы Ставропольского края»//Сборник законов и других правовых актов Ставропольского края от 30 марта 2005 г. №6 (156)

117.Закон РСФСР от 22.03.1991 N 948-1 «О конкуренции и ограничении монополистической деятельности на товарных рынках»/Бюллетень нормативных актов, февраль 1992 г. N 2

118.Уложение о наказаниях уголовных и исправительных. - Санкт-Петербург : Тип. 2 отд-ния собств. е. и. в. канцелярии, 1845. - [4], IV, 898, XVII с.

Материалы судебной и правоприменительной практики

119.Определение Верховного Суда РФ от 17 октября 2007 г. N 19-Г07-22 размещено на официальном сайте Верховного Суда. URL: http://www.vsrf.ru/index.php. (Дата обращения 31.10.2019)

120.Постановление Конституционного Суда РФ от 18 февраля 2000 года по делу о проверке конституционности пункта 2 статьи 5 Федерального закона «О прокуратуре Российской Федерации»//Собр. законодательства Рос. Федерации. 2000. № 9, ст. 1066.

121. Постановление Конституционного Суда РФ от 4 апреля 1996 г. N 9-П//Собрание законодательства РФ. 1996. No 16. Ст. 1909.

122.Определени Конституционного Суда РФ от 1 октября 1998 г. № 145-О «По запросу Законодательного Собрания Нижегородской области о проверке конституционности части первой статьи 6 Кодекса РСФСР об административных правонарушениях»//Собрание законодательства РФ. 1998. № 49. Ст. 6102.

123.О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности»: постановление Пленума Верховного Суда РФ от 20.09.2018 № 32. URL: http://www.vsrf.ru.

124.Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González. Case C-131/12. European court of human rights.

125.Klass and Others v. Germany, § 56, Series A, No 28. European court.

Научная и учебная литература

126.Андреева О.А. Региональная правовая политика преодоления экстремизма в молодежной среде: реалии и прогнозы // Государственная власть и местное самоуправление. 2014. N 9. С. 28 - 31.

127.Андриянов В.Н. Правовое регулирование безопасности личности в Российской Федерации // Основные направления государственной политики России в сфере обеспечения национальной безопасности: Материалы международной научно-практической конференции / Отв. ред. Е.М. Якимова. 2018. С. 13 - 19

128.Беларусь: Национальный ИКТ-профайл (Информационная безопасность и защита информации). URL: https://digital.report/belarus-informatsionnaya-bezopasnost/ (дата обращения: 02.12.2019).

129.Баранов А. А., Брижко В. М., Базанов Ю. К. Права человека и защита персональных данных. URL: http:/library.khpg.org/files/docs/Kn_L_.pdf дата обращения: 02.12.2019).

130.В Евросоюзе приняли новый закон о защите даннях. URL: https://threatpost.ru/v-evrosoyuze-prinyali-novyj-zakon-o-zashhite- dannyh/15749/ (дата обращения: 02.12.2019).

131.Варламова Н.В. Эффективность правового регулирования: переосмысление концепции // Правоведение. 2009. № 1. С. 200.

132.В Польше создали центр борьбы с российской пропагандой. :https://zaxid.net/u_polshhistvorili_tsentr_borotbi_z_rosiyskoyu_propagandoyu_n1424662 дата обращения: 02.12.2019).

133.Гнатюк С. Л. особенности защиты персональных данных в современном киберпространстве: правовые и технико-технологические аспекты: Аналитический доклад. К. : Нац. ин-т стратегических исследований, 2013. 51 с.

134.Грешневиков А.Н. Проблемы экологической безопасности России // Право и безопасность. URL: http://dpr.ru/pravo/pravo_16_21.htm. (Дата обращения 31.10.2019)

135.Гончаров И.В. Федеральное вмешательство в дела субъектов Федерации как средство обеспечения конституционной безопасности /А.И. Гончаров. - М.: Академия управления МВД России, 2003. С. 19.

136.Грибин Н.П., Диденко А.В. Концептуальные основы национальной безопасности Российской Федерации: Монография. М., 2010.

137.Жарова А.К. Право и информационные конфликты в информационно-телекоммуникационной сфере. М.: Янус-К, 2016. 246 с.

138.Злотникова Е.В. Ограничение демократических прав и свобод государства в период повышенной террористической угрозы: прихоть правительства или необходимость? // Государственное регулирование общественных отношений: электронный научный журнал. 2016. № 3 (17).

139.Затинайко О., Павленко В., Бочарников В., Свешников С. Политика безопасности и военно_политические отношения Венгрии. Наука и оборона. № 1. 2014. С. 9-18.

140.Европейский Суд по правам человека : материалы практики (2015-2016 гг). 2017. – 272 с.

141.Европарламент принял резолюцию с осуждением Венгрии. 438 URL: http://www.novayagazeta.ru/news/ 54209.html дата обращения: 02.12.2019).

142.Елфимова О.С. Национальная безопасность в теории и законодательстве России // Lex russica. 2016. N 10 (119). С. 15 - 27

143.Иоффе О.С. Юридические нормы: и человеческие поступки / О.С. Иоффе Акт. вопросы советского гражданского права. М.: Юрид. лит., 1964. С. 52-67.

144.Конституционный статус гражданина / [отв. ред. Б. Н. Топорнин]. М.: Наука, 1989. 205 с.

145.Квитко А.Ф. Конституционно-правовые основы ограничения прав и свобод человека и гражданина в Российской Федерации: Автореф. дис. ... канд. юрид. наук. М., 2007.

146.Комиссарова Е.Г. Защита профессиональной чести сотрудника полиции гражданско-правовыми средствами // Вестник Тюменского института повышения квалификации сотрудников МВД России. 2014. N 3. С. 110 - 115.

147.Калюжный А.Н. Федеральный закон «О безопасности»: итоги реализации и перспективы развития // Военно-юридический журнал. 2014. N 3. С. 7 - 10.

148.Кузнецова: объем детской порнографии в интернете за 5 лет вырос на 63%. [РИАН, 01.11.2016]. URL: https://ria.ru/society/20161101/1480448277.html (дата обращения: 31.10.2019)

149.Колоткина О.А., Ягофарова И.Д. Право личности на безопасность: к вопросу о расширении перечня конституционных прав и свобод // Законы России: опыт, анализ, практика. 2017. N 10. С. 94 - 96.

150.Костенко О. В. европейские стандарты правового регулирования оборота информации с ограниченным доступом в работе органов прокуратуры/ А. Костенко. серия «Право». Выпуск 34, том 3. 2015. С.109-114

151.Климчук О. О., Ткачук Н. А. Роль и место спецслужб и правоохранительных органов ведущих стран мира в национальных системах кибербезопасности. Информационная безопасность человека, общества, государства. 2015. № 3 (19). С. 75-83.

152.Лищина И. Ю. Международные механизмы защиты прав человека. 16 (57) / Лищина И. Ю. 2016. – 112 с

153.Малько А. В. Права человека в России и Европейская Конвенция о защите прав человека и основных свобод. Ч. 1 / А. В. Малько ; [отв. ред. В. И. Новоселов]. Саратов: Ин-т российского и международного права, 1997. 257 с.

154.Магденко А.Д. Национальные виды спорта: правовое регулирование в условиях глобализации // Научно-спортивный вестник Урала и Сибири. 2016. N 4(12). С. 65 - 69.

155.Молдова: Национальный ИКТ-профайл (Информационная безопасность и защита информации). URL: https://digital.report/moldova-informatsionnaya-bezopasnost/ (дата обращения: 02.12.2019).

156.Мнения экспертов Молдовы: Законопроекты в области информационной безопасности противоречат друг другу, то есть ведут к злоупотреблениям. URL: http://www.allmoldova.com/ru/project/mnenie/mnieniia-ekspiertov-moldovy- zakonoproiekty-v-oblasti-informatsionnoi-biezopasnosti-protivoriechat-drugh- drughu-to-iest-viedut-k-zloupotrieblieniiam (дата обращения 02.12.2019).

157.Нестеряк Ю. В. международные критерии информационной безопасности государства: теоретико-методологический анализ. Вестник НАДУ. № 3. 2013. С. 40-45

158.Осипов В.А. Правовые средства как элемент механизма обеспечения правовой безопасности общества // Закон и право. 2009. N 1. С. 12 - 14.

159.Петров Д.Е. Ограничение распространения информации в сети Интернет // Юридический мир. 2012. № 1. С. 32—34

160.Патрушев заявил о значительном росте числа несовершеннолетних наркоманов. [RBC.ru, 03.03.2017]. URL:

https://www.rbc.ru/rbcfreenews/58b9364c9a7947f2bb04d0c2 (дата обращения: 31.10.2019)

161.Персональные данные: новые правила в Европейском Союзе. URL: https://habrahabr.ru/post/300348/ (дата обращения: 02.12.2019).

162.Руснак А.К. Молдова и информационная безопасность. SECURITATEA INFORMATIONALĂ 2011: Conferinţa Internaţională, ediţia a VIII-a, 4 mai 2011. C.62-63.

163.Республика Хорватия // Гуманитарные технологии: Аналитический портал. URL: http://gtmarket.ru/ countries/croatia/ croatia-info (дата обращения: 02.12.2019).

164.Ряд VPN-сервисов отказались сотрудничать с Роскомнадзором. [SecurityLab, 09.11.2017]. URL: https://www.securitylab.ru/№ews/489585.php (дата обращения: 31.10.2019)

165.Распределение блокировок сайтов по ведомства. [Электронный ресурс]. Режим доступа: https://reestr.rublacklist.net/visual (дата обращения: 31.10.2019).

166.Страны СНГ будут сотрудничать в борьбе с киберпреступностью: URL: https://www.ritmeurasia.org/news--2017-08-28-- strany-sng-budut-sotrudnichat-v-borbe-s-kiberprestupnostu-32043 (дата обращения: 02.12.2019).

167.Сакович В.А., Бровка Г.М. Инновационная безопасность: основные понятия, сущность // Наука и техника. 2016. Т. 15. N 2. С. 144 - 153.

168.Стецовский Ю. И. Право на свободу и личную неприкосновенность: Нормы и действительность / Ю. И. Стецовский. М.: Дело, 2000. 720 с.

169.Туликов А.В. Информационная безопасность и права человека в условиях постиндустриального развития (теоретико-правовой анализ): дис. … канд. юрид. наук. М., 2017. 180 с.

170.Трусов Н.А. Правовое закрепление понятия и системы национальной безопасности России // Вестник Нижегородской академии МВД России. 2014. N 4 (28).

171.Устинов В. С. Теория и практика ограничения прав человека по российскому законодательству и международному праву. Ч. 1 / [под ред. В. М. Баранова]. Нижний Новгород: Нижегородский юрид. ин-т МВД РФ, 1998. 289 с.

172.Фомин А.А. Юридическая безопасность субъектов российского права. Саратов: Изд-во ГОУ ВПО «Саратовская государственная академия права», 2005;

173.Фатеев К.В. Военная безопасность Российской Федерации и правовые режимы ее обеспечения (теоретико-правовое исследование): Монография. М., 2004.

174.Число суицидов в России выросло почти на 60%.URL: https://www.vedomosti.ru/politics/news/2017/03/20/681840-chislo (дата обращения: 31.10.2019)

175.Шабуров А.С. Правовая безопасность в системе национальной безопасности // Вестник Южно-Уральского государственного университета. Серия: Право. 2015. Т. 15. N 3. С. 24 – 30.

176.Шайо А. Самоограничение власти (краткий курс конституционализма) / А. Шайо. М.: Юристъ, 2001. 307 с.

177.Шабуров А.С. Правовая безопасность в системе национальной безопасности // Вестник Южно-Уральского государственного университета. Серия: Право. 2015. Т. 15. N 3. С. 24.

178.Шигуров А.В. Нарушение конституционных прав граждан России «Антитеррористическим пакетом» И. Яровой // Мир науки и образования. 2016. № 4 (8). С. 32-38.

179.Шатун В. Т. Информационная безопасность – неотъемлемая составляющая национальной безопасности. 2016. Т. 267. Вып. 255. С. 174-180

180.Эбзеев Б. С. Ограничения конституционных прав: понятие и пределы / Б. С. Эбзеев 2015. С. 27-41.

181.Ягофарова И.Д. Право личности на безопасность: к вопросу о расширении перечня конституционных прав и свобод // Законы России: опыт, анализ, практика. 2017. N 10. С. 94 - 96.

182.Crounse S. The Fair Information Principles: A Comparison of U.S. and Canadian Privacy Policy as Applied to the Private Sector. NY: Rochester Institute of Technology, ProQuest, UMI Dissertations Publishing. 2009. 174 p.

183.Goncalves M.E., Jesus I.A. Security Policies and the Weakening of Personal Data Protection in the European Union // Computer Law and Security Review. 2013. No 29. P. 255–263.

184.Coudert F. When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies // Computer Law and Security Review 26 (2010). P. 381.

185.Verfassungsschutz (Bfv).URL: http://www. verfassungsschutz.de (дата обращ 02.12.2019).

186.Cyber-und Informationsraum: URL: http://cir. bundeswehr.de/portal/a/cir/start (дата обращения: 02.12.2019).

187.Politique de sécurité des systèmes d'information de l'état. Mode acces. URL: http://circulaire.legifrance.gouv.fr/pdf/2014/08/cir_38641.pdf (дата обращения: 02.12.2019).

188.Laura Chappell, Palgrave Macmillan. Germany, Poland and the Common Security and Defence Policy. Converging Security and Defence Perspectives in an Enlarged EU. 29 august 2012. 232 p.

189.Cyberintelligence. URL: https://www.sri.ro/ cyberintelligence- en.html. (дата обращения: 02.12.2019).

190.The Senate passed the draft low regarding the cyber security of Romania. URL: http://actmedia.ua/daily/the-senate-passed-the -draft-law- regarding-the ceber-security-of-romania/55734 (дата обращения: 02.12.2019).

191.Nigel Waters, Graham. Interpreting the Security Principle. URL: http://www.cyberlawcentre.org/ipp/wp/WP1%20Security.pdf (дата обращения: 02.12.2019).

192.L: http://oac.gov.by/ files/files/pravo/ukazi/Ukaz_129.htm. (дата обращения: 02.12.2019).

193.Publication du décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale. Mode 437 acces. URL: http://www.ssi.gouv.fr/actualite/publication-du-decret-n-2015-351- du-27-mars-2015-relatif-a-la-securite-des-systemes-dinformation-desoperateurs-dimportance-vitale (дата обращения: 02.12.2019)

194.Taking advantage of opportunities – avoiding risks. URL: https://www.bsi/bund.de//EN/Home/home_node.html$jsessionid= EA326461A185448F29C194C194C91BC85F23.2_cid286 (дата обращ: 02.12.2019).

195.The World Factbook: Central Intelligence Agency. URL: https://www.cia.gov/library/publications/the-world-factbook/fields/2144.html (дата обращения: 02.12.2019).