Санкт-Петербургский государственный университет

**НЕАРОНОВ Аким Андреевич**

**Выпускная квалификационная работа**

**Влияние политической коммуникации в сети Интернет на информационную безопасность Российской Федерации**

Уровень образования: магистратура

Направление 41.04.05 «Международные отношения»

Основная образовательная программа BM.5565. \* «Мировая политика»

 Научный руководитель:

 Кандидат политических наук

 доцент, Болгов Р. В.

 Рецензент:

Профессор кафедры международных отношений, Гуманитарный институт, Федеральное государственное автономное образовательное учреждение высшего образования

«Санкт-Петербургский политехнический университет Петра Великого»

Бахтуридзе З.З.

Санкт-Петербург

2019

**Содержание**

Введение…………………………………………………………………………………………………......3

Глава первая. Теоретико-методологическое обоснование информационной безопасности……......…7

1.1 Сущность информационной безопасности, в условиях глобального информационного обмена………………………………………………………………………………………………….….....7

1.2 Обоснование информационной составляющей национальной безопасности России....…...........14

1.3 Зарубежный опыт в области информационной безопасности - анализ практики США……...…..18

Глава вторая. Политическая коммуникация в сети Интернет, правовое обоснование обеспечения информационной безопасности Российской Федерации………………………………….....................26

2.1 Сеть Интернет как средство политической коммуникации………………………………….......…26

2.2 Система обеспечения информационной безопасности в Российской Федерации……………...…31

2.3 Применяемая нормативно-правовая база…………………………………………………...…......…34

2.4 Информационное воздействие как угроза социальному благополучию общества………..…..….40

Глава третья. Пути совершенствования и оптимизации обеспечения информационной безопасности, в условиях новейших течений………………………………………………………………………….....46

3.1 Обоснование основных направлений оптимизации обеспечения информационной безопасности в Российской Федерации………………………………………………………………………………….46

3.2 Совершенствование системы обеспечения информационной безопасности………...….…..……54

3.3 Освещение новейших течений в области политической коммуникации и информационного взаимодействия……………………………………………………………………………………….……59

Заключение…………………………………………………………………………………………..…….63

Список литературы…………………………………………………………………………………..……67

**Введение**

В настоящее время, обеспечение информационной безопасности государства, является одним
из важнейших аспектов его внешней и внутренней политики. Что обосновывает значимость исследования проблематики взаимосвязи политической коммуникации
в информационной сфере и информационной безопасностью государства.

Всемирная система объединенных компьютерных сетей для хранения, обработки и передачи информации - коммуникационная сеть Интернет являются самостоятельным пространством политических коммуникаций всех стран, на территории которых она функционирует. В современной системе «мирового баланса сил», государство, обладающее превосходством в информационном пространстве, посредством данного лидерства, получает глобальный информационный контроль над мировым сообществом и может навязывать свои ценности другим, менее информационно-развитым государствам, наращивать свое военное, политическое, геополитическое и экономическое влияние во всем мире. Страны, производящие и передающие информацию, которую воспринимает большинство населения планеты или же государства, осуществляющие контроль за материально–техническими ресурсами сети Интернет получают этим возможность по изменению баланса сил. Все участники глобального информационного обмена обеспечивают безопасность своих стран от угроз информационного воздействия. Особое значение исследованиям направлений информационной безопасности уделяют те страны, которые уже оказывают, или претендуют на оказание значительного влияния на глобальные политические процессы. Полностью это утверждение относится к Российской Федерации.

**Актуальность исследования:** Процесс сильнейшего развития коммуникаций в сети Интернет, являющийся закономерным последствием стремительного развития технологий, сформировал в мире единое информационное пространство, создание, которого, повлекло за собой тотальную унификацию информационных средств воздействия. Вышеописанные процессы указывают на глобализацию информационного пространства и развитии в нем новых форм политической борьбы и механизмов манипуляции общественным сознанием, а также на усложнение подсистем внутри политической системы каждого государства. Данные изменения, определяют приоритет проблемы в качестве задачи для политической практики и обосновывает актуальность научной проблемы. Стоит также отметить, что предмет исследования показывает устойчивые показатели по охвату аудитории на территории всех государств, при развитии технологий с тем же темпом, что и на данный момент, через 10 лет доступ к глобальному информационному обмену будет повсеместно на планете.

Аудитория Интернета на Май 2019 год составляет 4,39 миллиарда человек, на 9% больше, чем на год раньше. Согласно пакту отчетов о состоянии глобальной сети на 2019 год, подготовленный агентствами «We Are Social» и сервисом «Hootsuite», аудитория сети Интернет растет со скоростью 1 миллион новых пользователей каждые 24 часа.

На сегодняшний день информационно-коммуникационная сеть Интернет и объем генерируемой, хранимой и передаваемой информации, вкупе с мгновенной скоростью распространения увеличивают интенсивность её воздействия на аудиторию. Так же сетевые технологии дают обширное подспорье для социального контроля и реализации механизмов манипуляции.

Обладая влиянием на все области жизнедеятельности любых без исключения социальных групп всепроникающее информационно-коммуникационное поле, формируемое сетью Интернет, своим наличием, позволяет указать на угрозу манипуляции в нем общественным сознанием, что в контексте его глобализации и унификации, является прямой угрозой информационной безопасности государства, которая в свою очередь является угрозой национальной безопасности. Все ведущие страны и неправительственные акторы мировой политики и международного взаимодействия включили информационную угрозу в разряд основных, на ряду, с угрозами ядерной и экономической безопасности государств. Политическое руководство Российской Федерации, осознает важность и необходимость развития информационной безопасности. Основными векторами были выбраны: развитие информационно-телекоммуникационной инфраструктура, улучшение информационной среды, обеспечение безопасности в информационном обществе.

**Степень научной разработанности проблемы:** Информационное воздействие обладает высокой эффективностью, неограниченным количеством конечных адресатов и в контексте развития информационно-коммуникационных технологий – мгновенной скоростью передачи информации. Вышеуказанные факторы стали причинами интереса ученых и исследователей, как зарубежных, так и отечественных к проблематике взаимосвязи политической коммуникации в информационно-коммуникационной сети Интернет и информационной безопасностью государства. Автор обращается к работам Соловьева А.И[[1]](#footnote-1), Пуначева В.П[[2]](#footnote-2), Прокофьева В.Ф[[3]](#footnote-3), анализу также подвергаются работы Расторгуева С.П[[4]](#footnote-4) и Попова Г.Н[[5]](#footnote-5), обращаясь к зарубежным исследователям, автором были изучены работы следующих исследователей: Xin.Z[[6]](#footnote-6), O.V.Lankin[[7]](#footnote-7), а так же Nikishin K[[8]](#footnote-8), Jensen K[[9]](#footnote-9). Процесс глобальной информатизации, начался менее полувека назад и на данный момент прогресс его развития увеличивается с каждым днем. Именно по этой причине, невозможно точно спрогнозировать на долгосрочную перспективу угрозы, с которыми столкнется мировое сообщество, если одно из государств монополизирует право над управлением глобальной сетью мировой информаций, но данная тематика раскрывается в научных работах и исследованиях ученых на протяжении последних тридцати лет. В последние два десятилетия, аспекты воздействия сети Интернет на политическую коммуникацию и проблематика глобального информационного взаимодействия рассматривается более обширно и позволяет констатировать формирование отдельной области политических исследований.

Причем формирование более детальной темы исследований можно отметить не только в политической науке, но и в сфере юриспруденции и правотворчества, а также в области социологии и культурологии. В направлении современного политического знания – феномен политической коммуникации и горизонтальные связи данной проблематики является одним из приоритетных направлений.

Среди отечественных исследователей понятие «политической коммуникации» рассматривается в научных трудах Серебрянникова В.В[[10]](#footnote-10), поднимающего проблематику «избыточности» информации, Зиновьева П.В[[11]](#footnote-11) и Г.Почепцова[[12]](#footnote-12), в своих исследованиях политическую коммуникацию рассматривают как область обращения информации.

Задачу изучить и оценить информационно-коммуникационную сеть Интернет в своих научных работах перед собой ставят Д. Моррис, Л.Гроссман, С.Блэк, М.Г.Анохин, в то же время исследователи Проценко Е.В[[13]](#footnote-13) и Василенко Л.А[[14]](#footnote-14),утверждают, что политическая коммуникация в сети Интернет, выводит политический процесс на новый уровень.

**Нормативно-правовую базу исследования** составляет: Доктрина информационной безопасности РФ (1996,2000,2009 гг)[[15]](#footnote-15), Указ Президента РФ № 537 от 12 мая 2009 «Стратегия национальной безопасности Российской Федерации до 2020 года»[[16]](#footnote-16), Федеральная целевая программа «Электронная Россия», Программа «Информационное общество 2011-2020 г)[[17]](#footnote-17).

**Предметом исследования** является содержание государственной политики в области информационной безопасности Российской Федерации при политической коммуникации в информационно-коммуникационной сети Интернет.

**Основными методами исследования**, в рамках данной исследовательской работы стали: наблюдение, анализ, экспертная оценка и логическое моделирование.

**Цель исследования** состоит в определении основных направлений оптимизации государственной политики в области обеспечения информационной безопасности политической коммуникации.

**Задачи исследования**

- выявить приоритетные направления по обеспечению информационной безопасности Российской Федерации

-рассмотреть роль информационно-коммуникационной сети Интернет в системе безопасности государства.

 - выявить основные проблемы, ведущие к отставанию в информационном поле от лидирующих в этой области государств.

- проанализировать новейшие угрозы в области информационного взаимодействия.
**Объем и структура работы**. Диссертация состоит их трех глав, десяти параграфов, введения, заключения и списка использованной литературы и источников.

**Глава первая**

**Теоретико-методологическое обоснование информационной безопасности.**

**1.1 Сущность информационной безопасности, в условиях глобального
информационного обмена.**

Информационная безопасность - это комплекс мер по защите государства, общества и личности от информационного оружия. Под информационным оружием подразумевают средства нападения на информационные сети, электронный шпионаж, вирусы, способные влиять на мировую экономическую ситуацию или даже разрушать ключевые информационные системы. Данное оружие дешево в производстве и сложно в обнаружении, что делает его особенно привлекательным для преступников[[18]](#footnote-18). В вопросах национальной безопасности государства наступает новый этап, когда противостояние развертывается в информационном поле. Происходит переход от привычных видов оружия к избирательному, точечному воздействию с помощью современных технологий.

Для современного общества Российской Федерации важно освоить информационную сферу, как социальную. Изучить её влияние как на личность, так и на отдельные социальные группы, чтобы в дальнейшем иметь возможность регулировать и управлять данным влиянием. В противном случае информатизация общества будет развиваться стихийно и неподконтрольно гражданам, а при подобном сценарии безопасность, как личности, так и общества в целом будет под угрозой. Без понимания принципов работы современных средств коммуникации, в условиях политической нестабильности и экономического кризиса невозможно управление социально-политическими процессами в стране, а именно от них в большей степени зависит благополучие государства и место Российской Федерации в мировой цивилизации в будущем.

 Бывший министр по связи и информатизации Российской Федерации Л.Д.Рейман[[19]](#footnote-19) в своём докладе на семинаре «Глобализация информационного пространства вызовы и новые возможности для России» дал характеристику глобального информационного пространства:

«Конец XX века ознаменовался огромным прогрессом в развитии телекоммуникационных технологий, Сегодня, тридцать лет спустя после создания первых компьютерных сетей и восемь лет спустя после того, как Интернет приобрел современные очертания, говорить о глобальном информационном пространстве стало не только теоретически интересно, но и практически необходимо. Пятьдесят лет тому назад, если вы хотели переслать 30 страниц текста на расстояние 5 тысяч километров, вам потребовалось бы примерно 10 дней, и стоило бы это около 30 долларов за услуги почтовой связи. Двадцать лет тому назад вы бы, наверное, прибегли к услугам факса. Это заняло бы у вас примерно 1 час, и стоимость составляла где-нибудь 50 долларов. Сегодня, если говорить о самых лучших сетях передачи данных, на это требуется не более 3 секунд, а стоимость составит около 3 центов. Таким образом, стоимость упала в 1000 раз, скорость возросла в 300 тысяч раз. Колоссальное увеличение скорости при одновременном снижении стоимости, появление практической возможности передачи мультимедийной информации в реальное время, увеличение скорости систем поиска и обработки информации в миллион раз – это основы будущего развития всех сфер жизни общества». По скорости передачи информации и количеству конечных адресатов, современные информационные технологии передачи данных, во много раз превосходят привычные информационные сети: радио, телевидение и т.д. Становится ясно, что сеть Интернет может использоваться как способ влияния и воздействия на граждан. Число пользователей с каждым днем увеличивается, все больше компаний, фирм, институтов, государственных предприятий и даже военных объектов подключаются к единой мировой информационной сфере.

Научные труды многих исследователей, среди которых: Прайс М[[20]](#footnote-20), Попов Г.Н[[21]](#footnote-21) и Kresimir S.[[22]](#footnote-22) указывают на формирование информационного общества, как следствие распространение информационных технологий, а также на динамику отношений между странами и повышение общий уровень образования населения, как признаки информационного общества. Катализатором становления информационного общества является глобализация, придавая информационным технологиям огромный ресурсный и организационный потенциал.

Информационное общество обладает тремя ярко выраженными признаками.

1) Взаимоотношения между обществом и естественным природным ресурсом планеты выстраиваются на основе информации, а не на основе опыта и эмпирического исследования.

2) Информационная модель государства, критерий еще 40 лет назад проистекающий из выстроенной идеологической внутренней государственной модели, на сегодняшний день создается на основе информации, создание и дополнение которой возможно любому участнику информационно-коммуникационного взаимодействия.

3) Для субъектов государственной власти, являющимися субъектами властных отношений, как во внутренней, так и во внешней информационной среде – скорость и качество обработки информации стало ключевым и решающим критерием успешного функционирования.

Информационная сфера, развиваясь, образовывает глобальные информационные ресурсы, подконтрольные как межгосударственным корпорациям, так и отдельным государствам. Являясь таким образом производителями информации, для неограниченного количества потребителей.

Определение «информационной безопасности государства» также трактуется, как «состояние защищенности ее национальных интересов в информационной сфере», состояние «защищенности от угроз» в информационной сфере, определяется совокупностью интересов личности, общества и государства и их подверженности внутренним и внешним угрозам.
В данной работе объектом информационной безопасности, является государство, определенное конкретными свойствами, среди них: наличие аппарата власти, выделенного из общества, наличие суверенитета, разделение населения по территориальным единицам. А также в контексте данного исследования: высокий уровень информатизации и обеспечения доступа к информационно-коммуникационной сети Интернет на всей территории выбранного государства, в данном случае Российской Федерации. Любые сферы жизнедеятельности современного государства и общества в нем подвержены информационному влиянию. За исключением особых «рекреационных» или «резервационных» зон, во всех социальных стратах, обществах, организациях, и личностях потребление и производство информации неразрывно связано с всемирной сетью Интернет. Возможности, доступные, благодаря сверхбыстрому транслированию информации на любые расстояния, колоссальным вычислительным мощностям современных компьютерных систем, а также простоте и унифицированности информации[[23]](#footnote-23), доступом к которой обладает уже большая часть населения планеты, могут быть использованы не только во благо. Подобные ресурсы и возможности, которые они дают, могут и регулярно используются во вред интересам личности, общества и государства[[24]](#footnote-24).

Всеобъемлющее проникновение информационных технологий в систему обеспечивающую функционирование жизненно важных элементов современного общества, а во многом и сотворение данной системы исключительно на базе современных технологий. Обуславливает необходимость не только защиты информации от несанкционированного доступа, но и защиты технических и электронных систем, поскольку прекращение их функционирования может вызвать технические сбои и аварии, которые повлекут за собой человеческие жертвы, следовательно, в сфере применения автоматизированных технологий, роль безопасности осуществляемого процесса становится главенствующей. По этой, наряду с другими причинами роль информационной безопасности в системе национальной безопасности, как Российской Федерации, так и других, лидирующих на политической арене, стран, увеличивается
с каждым годом, а в отдельных примерах, даже занимает ключевое место[[25]](#footnote-25).

В Российской Федерации наступает новый этап развития системы обмена информации, повсеместное внедрение информационно-коммуникационных технологий[[26]](#footnote-26), распространение сетей глобального и корпоративного масштаба, предоставляет возможности для повсеместного и широкополосного информационного обмена. Данный аспект развития государства дает первостепенную значимость обеспечению информационной безопасности, актуальность которой обозначена следующими факторами:

• Повсеместное возрастание количества персональных компьютеров (ПК), применяемых во всех областях, в том числе военной, строительной и экономической, следствием чего является вовлечение государственных институтов в общую информационную сферу.

• Увеличение объемов информации, регистрируемой, обрабатываемой с помощью ПК.

• Развитие передовых технологий, расширяющих возможность нарушения информационной безопасности в новых, до этого не изученных сферах и отставание в этой среде технологий направленных на защиту, противодействие преступным действиям.

• Созданное, единое информационное пространство на базе сети Интернет, объем и размер, которого настолько велик, что суммарные действия всех государств по противодействию преступлениям в информационной сфере, не может обеспечить необходимый уровень информационной безопасности.

Наступает новый этап развития системы обмена информации, повсеместное внедрение информационно-коммуникационных технологий, распространение сетей глобального и трансконтинентального масштаба, предоставление возможности участия в глобальном информационном взаимодействии. Для Российской Федерации, государства, претендующего на роль сверхдержавы в современном мире, значение информационной безопасности сложно переоценить и опасно недооценивать.

Информационно-коммуникационные сети связывают все отрасли безопасности, промышленности, социальной и экономической сферы, а также на прямую влияют на формирование политической и социальной позиции граждан.

Решение проблем и предопределение и нейтрализация угроз в области информационной безопасности осуществляется государственной политикой в области информационной безопасности. Государственная политика Российской Федерации, касательно информационной безопасности возможна только при согласованных действиях всех элементов системы обеспечения информационной безопасности и реализуется, исходя из следующих принципов.

1. Безусловное равенство для всех участников процесса информационного взаимодействие. Государственная политика, путем разработки нового законодательства, формирования нормативно-правовой базы информационных связей в обществе, для обеспечения равенства среди участников вне зависимости от их статуса, местонахождения или других различий.
2. Создание современных информационно-коммуникационных сетей, телекоммуникационных технологий и информационных средств, способных обеспечить создание отечественных информационно-коммуникационных сетей, охватывающие акторов информационного взаимодействия, как внутри государства, так и включение данных сетей в мировые информационные сети.
3. Государство исходит из того, что с помощью информационно-коммуникационных сетей, генерируются ресурсы, в том числе интеллектуальная собственность, создаваемая участниками информационного взаимодействия, которые являются объектом собственности и имеет материальную ценность, несмотря на нематериальное расположение.
4. Государственная политика не допускает монополизма в области информационно-коммуникационных сетей. Государство принимает согласованные решения, рассмотренные коллегиально, органами власти, местного самоуправления и обществом.

 Обеспечение информационной безопасности Российской Федерации должно быть всеобъемлющим и интегрированным в единое технологическое сотрудничество в масштабах страны. Потеря государственного контроля над информационной сферой станет причиной дезорганизации всех сфер общественной жизни.

Обосновав необходимость информационной безопасности и основные принципы государственной политики по её реализации, необходимо осветить основные требования к системе, обеспечивающей информационную безопасность Российской Федерации, а именно:

 - надежность функционирования информационно-коммуникационной сферы, обеспечивающий стабильный режим работы.

 - достоверность сведений о состоянии нформационно коммуникационной системы,
а также сведений относящихся к её подсистеме.

- по своему содержанию, важно наличие информации, способствующей консолидации всех слоев социума вокруг морально-культурных ценностей, привычных и исторически сложившихся в российском обществе.

 - быстрый и качественный анализ информации, обеспечение структур субъекта информацией обладающей достаточным уровнем достоверности, оперативности, полноты, доступности, конструктивности и рассматривающей объект информации с многих сторон.

 - субъекта информационно-коммуникационной сферы доступом к информационному ресурсу системы, который в свою очередь является удобным, простым, надежным и доступным в любое время.

Раскрыв определение таких понятий, как: информационная безопасность государства и информационная сфера в рамках данного исследования следует раскрыть понятие: «угроза» или «опасность» информационного обмена. Обращаясь к нормативно правовой документации, в частности к Закону Российской Федерации «О безопасности»[[27]](#footnote-27), автор выделяет определение угрозе безопасности, как «совокупности условий и факторов, влекущих за собой опасность жизненно важным интересам личности, общества и государства. Классификация угроз определяется степенью конечного формирования угрозы. Что помогает разделить угрозы на «реальные» и «потенциальные»[[28]](#footnote-28).

 Реальная угроза – есть сформировавшееся, явление, обладающее высокой долей вероятности нанесения ущерба разного масштаба и вида, для наступления которого не достает нескольких условий.

Потенциальная угроза – есть лишь формирование предпосылок, возможных ситуаций или систем взаимодействий, итогом которых станет формирование реальной угрозы и нанесения вреда, как закономерного итога и результата реальной угрозы.

В рамках рассмотрения понятия информационная безопасность Российской Федерации и обоснования определения «угрозы», как «совокупности условий угрожающим интересам государства», является необходимым раскрыть понятие «интереса государства», в информационной сфере. В рамках данной исследовательской работы, обратившись к «Доктрине информационной безопасности Российской Федерации», автор выделяет три направления национальных интересов в информационной сфере:

Первое: Необходимость соблюдения и обеспечения достаточного уровня информационной безопасности конституционных прав и свобод граждан при получении, хранении, производства и использовании информации по средствам информационно-коммуникационных технологий. Следует отметить важность сохранения и укрепления традиций, ценностей и устоев, сформировавшихся в российском обществе, укрепление патриотизма среди населения, формирование здравой политической и социально-бытовой позиции граждан, посредствам достоверных и компетентных источников информации.

Второе: Информационное обеспечение государственной политики Российской Федерации должно подкрепляться достоверной информацией, доводимой до сведения российской и мировой общественности – открыто и без искажений. Подобное обеспечение должно освещать официальную позицию и актуальную информацию по вопросам, имеющим социально-политическое влияние и значимость.

Третье: Стоит отметить невозможность обеспечение достаточного уровня информационной безопасности, а как следствие и отражение реальных или потенциальных угроз для национальных интересов государства в информационной сфере без надлежащего и достаточного уровня материально-технического обеспечения. Исходя из данного утверждения, в рамки национальных интересов входит развитие новых информационно-коммуникационных технологий, увеличение производственных и трудовых мощностей в области информационно-коммуникационных технологий и области высокотехнологичного производства, создание возможностей для обеспечения, сперва внутреннего рынка средствами информатизации и их производными, а в дальнейшем и рынка других государств.

Обосновав основные понятия, автор делает вывод о их взаимосвязанности, взаимообусловленности и достаточности для исследования в контексте данной исследовательской работы.

Информационное развитие современных технологий вызывает глобальные трансформации, которой подвержены все слои общества всех государств, вовлеченных в информационный обмен. Механизмы обеспечения информационной безопасности, также, как и инструменты информационного воздействия совершенствуются с каждым днем. Аудитория сети Интернет пополняется 1 миллионом новых пользователей каждые сутки. Угрозами для обеспечения информационной безопасности современного российского общества является активизация источников и обострение как существующих, так и новейших механизмов информационного противоборства. В условиях глобального информационного взаимодействия, информационная безопасность становится основным компонентом системы безопасности государственных и политических институтов общества, значит и системы национальной безопасности страны.

**1.2 Обоснование информационной составляющей национальной безопасности.**

Национальная безопасность – понятие многогранное и всеобъемлющее. В данной работе оно рассматривается через призму информационной безопасности и в ключе информационно-коммуникационных и сетевых угроз.

В современных условиях необходимо предвидеть и реальные и потенциальные угрозы и брать в расчет экономические, правовые, и многие другие аспекты для достижения необходимого уровня безопасности. Для обеспечения данных критериев безопасности необходимо непрерывно получать достоверную и полную информацию об угрозах и опасностях. Более того, необходимо генерировать информацию о возможностях устранения или нейтрализации подобных угроз в кратчайшие сроки. Это дает нам понять, что проблема обеспечения своевременного и полного уровня национальной безопасности, только на первый взгляд техническая задача, в ней, как и в любой другой многоуровневой системе присутствуют социально-политические, экономические и социокультурные элементы. Для государства могут повлечь разрушительные последствия наличие или отсутствие информации и её верного использования[[29]](#footnote-29). Информационное воздействие, осуществляемое посредствам сети Интернет, обладает огромным влиянием на общественное сознание. Обеспечение информационной защиты от влияния, которое могут распространить на наших соотечественников специальные формирования других стран[[30]](#footnote-30), ровно, как и акторы негосударственного типа, является одной из приоритетных задач национальной безопасности[[31]](#footnote-31).

 В данном контексте национальная безопасность Российской Федерации становится объектом информационного обеспечения государства. Этот тезис подводит нас к необходимости уточнить само понятие «национальная безопасность», определить наличии информационных связей, расширенных информационно-коммуникационных сетей и информационных сфер в контексте национальной безопасности страны.

Понятие «национальная безопасность» вошло в политико-правовой язык России в середине 90-х гг. ХХ столетия. Сам термин «национальная безопасность» на законодательном уровне был использован в Федеральном законе «Об информации, информатизации и защите информации от 20 февраля 1995г №24-ФЗ (утратил силу), а его определение закреплено в июле 1996г в Послании Президента РФ «О национальной безопасности».

«Национальная безопасность – безопасность её многонационального народа как носителя суверенитета и единственного источника власти в Российской Федерации[[32]](#footnote-32). Так же национальную безопасность можно определить, как состояние защищенности национальных интересов страны.»

«Угроза национальной безопасности – это совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам.»

Вышеизложенное помогает нам трактовать это понятие и выделить два главных направления для обеспечения национальной безопасности Российской Федерации.

а) Защита от угроз и опасностей б) создание необходимых условий для существования и надежного развития страны.

Первое направление предполагает организацию системы противодействия угрозам и опасностям и контроль за её функционированием. Второе же – необходимую деятельность по сохранению и преумножению материально-духовных потенциалов и ресурсов, а так же использование их для реализации в государственных интересах[[33]](#footnote-33). Для обеспечения достаточного уровня национальной безопасности необходимо определить субъекты и объекты национальной безопасности, нуждающиеся в информации.

Подобный подход к национальной безопасности государства демонстрирует нам неотъемлемость информационных процессов. Состояние безопасности или защищенности всегда связано с обладанием соответствующей информацией. Например: степень угрозы или опасности, возможности устранения или ликвидации последствий и т.д

При разработке общей характеристики национальной безопасности Российской Федерации, необходимо обратить внимание на некоторые особенности нашего государства.

Во-первых, система национальной безопасности Российской Федерации существует в условиях снижения антагонизмов как в международных отношениях с западными партнерами, так и с большинством стран бывшего СССР. Эпоха биполярно устроенного мира подходит к концу. На геополитической карте появляются все новые и новые центры силы, региональные и национальные интересы России оказывают существенное влияние на выбор внешнеполитической стратегии и долгосрочного планирования. Российская Федерация еще не до конца определила свое место в системе глобальной безопасности, ввиду своего геополитического положения, в будущем наше государство может занять место, столь необходимого «буфера» в отношениях между Западными и Восточными державами. Подобное положение напрямую влияет на информационную составляющую национальной безопасности России.

В первую очередь – информационное пространство России трансформируется. Распад Советского Союза, оказался катастрофой не только техно-социального, но и информационного класса. Общество оказалось разобщено, подавлено и в условиях отсутствия моральных и духовных ориентиров, угроза оказания влияния и манипуляций из вне стала реальной. Прежде замкнутое внутри СССР информационное пространство нашей страны, интегрируется в единую, международную информационную сферу.

Во-вторых, национальная безопасность Российской Федерации была и будет тесно связана с обеспечением безопасности стран бывших республик, образованных на территории СССР. Некоторые из них, к сожалению, были выведены из ареола влияния Москвы, но многие (например, Белоруссия, Казахстан, Киргизия и др.) желают тесного союза с Россией и образование единого защищенного информационного пространства является приоритетной задачей, которая окажет положительное влияние на развитие вопросов обеспечения коллективной и национальной безопасности. Подобные инициативы уже были реализованы в международном праве, Содружество Независимых Государств (СНГ) и Договор о коллективной безопасности (ДКБ), ставит перед Российской Федерацией задачу по обеспечению не только собственной национальной безопасности, но и коллективной безопасности стран участниц
СНГ и ДКБ . Стоит отметить, что ряд стран, тяготеющих к Западной Европе и США, следовательно, подвластных информационному влиянию, все чаще поднимают вопрос о вступлении в НАТО. В данной ситуации, общие информационные средства обеспечения, доставшиеся в «наследство» от СССР, всем вновь образованным на его территории странам повышают угрозу несанкционированного доступа к информации в информационных системах России.

В-третьих, современное становление системы национальной безопасности
Российской Федерации, совершается, в условиях зарождения новой российской государственности, которая в свою очередь формирует систему новых общественных отношений. Помимо сильнейшего давления оказываемого на наше государство извне, внутренняя политика России, характеризуется трудными взаимоотношениями между отдельными субъектами Федерации. Обеспечивать достаточный уровень национальной безопасности крайне необходимо, особенно в современных условиях внутренней нестабильности, кризиса экономики и социального расслоения. Стоит осознавать реальные риски по информационному воздействию, направленному на разжигание внутри российского общества конфликтов на этнической, социальной или религиозной почве.

Одним из направлений информационного воздействия на политику обеспечения национальной безопасности, является механизм информационного противоборства, ввиду используемых им механизмов, он относится больше к инструментам «мягкой», нежели «жесткой» силы, но последствия подобного противоборства, могут быть весьма разрушительны, что размывает в данном механизме границы между войной и миром, делая его частью информационной войны.

Основными угрозами, исходящими от механизма информационного противоборства, для национальной безопасности государства, подвергшегося подобному информационному акту воздействия со стороны другого государства, могут стать:

- создание атмосферы напряженности в обществе, дестабилизация социальной обстановки, провоцирование противоправных и неконституционных процессов.

- подрыв международного авторитета государства, деструктивное влияние на международные связи с другими государствами

- нарушения в системе управления войск, объектов военной и гражданской инфраструктуры.

- затруднение принятия решений органами как местного, так и федерального государственного управления

- дискредитация как отдельных лидеров государства, так и целых органов власти.

- спроектированный государственный переворот.

- инициирование массовых акций экономического, социального, трудового или иного организованного протеста

Наступивший новейший этап развития системы обмена информации, повсеместное внедрение информационно-коммуникационных технологий, распространение сетей глобального, локального и корпоративного масштаба, открывает возможности повсеместного и широкополосного информационного обмена. На сегодняшний день активность человеческих ресурсов зависит от информатизации и уровня внедрения технологических средств. Информация и информационные ресурсы стали ключевыми факторами развития государства, одновременно являясь новой формой ресурсов: информация может являться как товаром, так и производственной силой, как средством защиты, так и нападения.
В настоящее время большинство государств, использует информационную сферу, как для реализации, так и для защиты своих национальных интересов[[34]](#footnote-34).

**1.3 Зарубежный опыт в области обеспечения информационной безопасности – анализ практики США.**

Рассматривая вопрос информационной безопасности в глобальной информационной сфере невозможно не освятить опыт других государств. Лидером информатизации процессов, развития информационно-коммуникационных технологий, а также доминирующей страной по уровню влияния в глобальном информационной сфере, являются Соединенные Штаты Америки. В 1994 году Объединенная комиссия по безопасности опубликовала доклад, в котором говорится: «Информационные технологии – есть инструмент обеспечения решений геополитических кризисов, без единого выстрела. Политика обеспечения национальной безопасности и процедуры её реализации, должны быть направлены на защиту наших возможностей по ведению информационных войн и на создание всех необходимых условий для воспрещения противоборствующим США государствам вести подобные войны»[[35]](#footnote-35). Стоит отметить что уже в 1994 году, правительство и высшие эшелоны власти США осознавали важность и значимость информационно-коммуникационных технологий и возможностей, которые они открывают для внешней и внутренней политики. В решении современных политических и геополитических конфликтов информационное воздействие оказывает первостепенную и зачастую решающую роль. Вышеуказанная выдержка из доклада полностью описывает исключительную роль, которую информационное воздействие может оказать, применяясь в ситуациях конфликта между государствами и их интересами, а именно предоставить заведомо лучшую позицию еще до переломного момента применения грубой силы.

Помимо роли исключительного инструмента для решения возникающих в ходе реализации внешней политики ситуаций, информационное воздействие обладает, огромным потенциалом по трансляции идеалов и ценностей среди населения. Так в 1997 году, в документе «Стратегия национальной безопасности США в следующем столетии» представленному американскому конгрессу транслирование ценностей США за пределы своих государственных границ приравнивается к основному из тезисов, на котором базируется стратегия: «Лидирующая роль США подкрепляется силой демократических идеалов и ценностей. Мы исходим из того, что распространение демократии укрепляет американские ценности и повышает нашу безопасность и благосостояние. Следовательно, тенденция к демократизации и распространению свободных рынков по всему миру способствует продвижению американских интересов»[[36]](#footnote-36)

Стоит отметить, что, говоря о глобальной системе безопасности, специалисты из США не оперируют терминами устойчивого развития, глобальной стабильности, международного взаимодействия или партнерских отношений между государствами. Основное внимание определенно на продвижение собственных интересов и укреплению благосостояния США[[37]](#footnote-37). При анализе геополитических конфликтов, за промежуток времени в последние 25 лет, с момента публикации данного документа и утверждении его. Методом анализа документов, можно составить прямую взаимосвязь между государствами, впавшими в глубокий политический кризис и информационных компаний США об отсутствии, в подобных государствах демократического режима.

Информационное воздействие, оказываемое на государства Соединенными Штатами Америки не направленно на разрешение этнических, политических или военных конфликтов в отдельно взятых государствах. Оно направленно на удовлетворение национальных интересов США, будь то ресурсы на территории суверенных государств, предоставленные Американским компаниям в результате геополитическое влияния США в регионе.

Или же введение военного контингента на территорию суверенного государства с получением, а чаще и без получения соответствующей резолюции ООН. Предпосылками к подобным операциям «по обеспечению мира» всегда является обширная информационной компания[[38]](#footnote-38)[[39]](#footnote-39), освещающая действующее политическое руководство страны, на чью территорию совершается интервенция в свете «не демократических лидеров» и «диктаторов». Но причина лишь в том, что политические лидеры осуществляют политику, идущую в разрез с геополитическими планами США. Примеров за последние двадцать пять лет можно назвать много: Югославия, Ирак, Йемен, Гаити, Афганистан, Ливия, Сирия. И это только список стран, в которых было реализовано военное присутствие США, под эгидой стремления установить в суверенных государствах демократический режим. Стоит ли говорить, что ни одна из стран, где были проведены военные «демократические» военные операции США и их союзников, так и не смогли вернуться к стабильности и развитию. Не говоря уже про формирование устойчивых политических институтов.

 В случае если насильственный путь свержения власти, путем информационной поддержки государственного переворота или одобрения военной интервенции не реализуется, тогда «неугодному» государству, совершается предоставление кредитов организацией, в которой США принадлежит большинство голосов: Международным Валютным Фондом, а условия кредитования включают в себя выполнение условий договора о кредитовании, среди которых: предоставление стране активов, в условной валюте, возвращать которую необходимо резервной валютой МВФ, то есть американским долларом. Помимо этого, на территорию стран, в которых разыгрывается подобный сценарий массово заходят транснациональные корпорации. Механизм максимизации прибыли всегда один и тот же: первое время после появления на рынке ТНК-агенты осуществляют торговлю по цене ниже себестоимости товаров, восполняя издержки за счет прибыли из других филиалов. Подобная ценовая политика в течении короткого срока делает невозможным местное производство, закрываются предприятия, фабрики, заводы. Как только уровень производства в стране падает, цены возвращаются к привычным, а зачастую становятся еще больше. В экономике государства наступает стагнация и развал, что приводит к тому, что страна не может рассчитаться с МВФ и вынуждена брать новый кредит. Круг замкнулся. А предоставление подобных кредитных линий государствам преподносится в информационной сфере как ярчайший акт демократии и абсолютное достижение мирового сообщества.

В конце 1998 года Комитет начальников штабов ВС США издал Доктрину проведения информационных операций, где был подтвержден факт проведением американскими военными информационных операций наступательного характера. Более того в документе отмечалось, что возможность и осуществление подобных операций возможно, как в военное, так и мирное время.

Уже к 2005 году, согласно данным ФАПСИ Федерального агентства правительственной связи и информации при Президенте РФ, среди всех программ по вооружению в США, первое место занимают расходы на приобретение средств информационной борьбы и составляют более 18 млрд. долларов. Дополнительно отмечалось, что США уже имеют и активно создают новые центры глобального информационного воздействия на информационно-психологическую среду всего мирового сообщества.

Стоит отметить что спустя 15 лет, в планируемом военном бюджете США на 2020 год[[40]](#footnote-40), финансирование информационных средств противодействия, которые в новых документах описываются терминами «кибервоздействие» и «киберпротсранство», а также в данной статье расходов имеются и вовсе не определенные понятия, такие как «защита нации». Общая статья расходов носит название «кибербезопасность» и на 2020 год ориентировочный объем запрашиваемых средств составляет 9.6 млрд долларов[[41]](#footnote-41). Больше только у статьи «Космические войска». Вышеописанные факты, позволяют нам понять, что даже спустя много лет вопросы информационного воздействия остаются ключевыми и активно развиваются в США. Более того, специалистами Соединенных Штатов Америки активно ведется подготовка, как теоретическая, так и практическая специальных подразделений, чей профиль будут составлять исключительно операции по информационному воздействию.

Риторика Соединенных Штатов относительно собственной уникальности и исключительности никогда не была нова. Наши заокеанские партнеры неоднократно величали себя и «носителями демократии» и «шерифами Земли», стоит понимать, что как в вопросах реализации собственных национальных интересов, так и в вопросе информационного воздействия США не будет идти на компромисс. США воспринимает Российскую Федерацию, как угрозу своим интересам и национальной безопасности, что было подтверждено в Доктрине Национальной Безопасности США 2018, где Россия, возведена в разряд угроз наряду с Северной Кореей и Исламским Государством Ирака и Леванта (запрещена на территории Российской Федерации). Исходя из этого информационная политика США всегда будет направлена на дискредитацию позиций и исторических данных относительно Российской Федерации Уже на сегодняшний день, можно констатировать факт повсеместного уменьшения информированности среди Американского и Европейского населения фактов и результатов Второй Мировой Войны.
Информация, публикуемая относительно России в западно-американском сегменте сети Интернет, в настоящее время носит исключительно отрицательный характер и направленность. Обоснованием тому служит источник власти над сетью Интернет. Прообразом интернета является сеть ARPANET, которая была создана Агентством министерства обороны Соединенных Штатов Америки по перспективным исследованиям (DARPA). Процесс передачи данных, который осуществлялся внутри данной сети требовал систематизации и контроля, роль подобного регулятора возложили на команду исследователей из Калифорнийского университета. Говоря о «создателях» или «управленцах» глобальной сети, невозможно не указывать их. Один из них Джонатан Постел был руководителем направления, которое разработало сетевые протоколы, которые до сих пор используются в привычной нам сети Интернет. А сам Джонатан был первым администратором ARPANET. Благодаря его работе, были открыты и внедрены такие процессы как буквенные обозначения ресурсов (доменные имена), то что сейчас называется именем сайта, была сформирована и опробована на практике система IP-адресов.

На первых этапах становления Интернета, право на регистрацию и контроль за использованием доменных имен монопольно принадлежало компании Network Solution. Ввиду того, что ресурс и количество пользователей сети неуклонно росло, в 1998 году в США была сформирована Корпорация по управлению доменными именами и IP-адресами (ICANN), структура данной корпорации представляла собой некоммерческую, а совет директоров был выборным. Помимо администрирования данная организация совместно с инженерным советом интернета США (IEFT), занималась развитием и построением системы взаимодействия и архитектуры глобальной сети, результаты их деятельности мы видим сегодня в виде сформировавшейся глобальной коммуникационной сети Интернет. Правительство Соединенных Штатов, от лица Министерства торговли заключило с Корпорацией по управлению доменными именами и IP-адресами контракт, одним из условий которого было предоставлению Министерству торговли место в комитете Корпорации, что автоматически давало право вето на принимаемые решения, следовательно, ни одно решение корпорации, которая занималась разработкой и созданием интернета, каким мы его сейчас видим не могло быть принято без одобрения с правительством США. Спустя много лет, с развитием коммуникационной сети и охватом всего мира, было организованно и сформировано пять региональных регистраторов, которым корпорация ICANN делегировала свои полномочия, избирая их по принципу территориальной расположенности и лояльности. Весь объем информации, которая хранится, генерируется, передается или используется в российском сегменте Интернета - обслуживается аккредитованным регистратором «RIPE NCC», офисы которой, расположены в Амстердаме и Дубае. Контракт между Правительством США в лице Министерства торговли и Корпорацией ICANN регулярно продлевался, несмотря на то, что многие пионеры интернета, такие как разработчик протоколов ARPANET Стив Крокер еще с 2000х годов заявляли, что контроль над интернетом необходимо передать в руки международного сообщества.

Сосредоточение инструментов влияния и механизмов управления сетью Интернет в руках одного государства имеет весьма ощутимые угрозы для безопасности других стран. В случае резкого обострения международной обстановки, или же банально в случае, если США преследуя свои собственные интересы, пожелают нанести деструктивное воздействие на другие страны, они могут воспользоваться своим влиянием на ICANN, что в свою очередь нарушит работу национальных сегментов коммуникационной сети Интернет.[[42]](#footnote-42) Или же возможно лишение государств их доменов верхнего уровня, таких как российский: «.ru» или китайский: «.cn.» Преследуя цели обеспечения информационной безопасности от подобного вида угроз, министр связи Российской Федерации Николай Никифоров анонсировал создание дублирующих элементов инфраструктуры коммуникационной сети Интернет. Китай уделяет внимание информационной безопасности на протяжении последних 25 лет[[43]](#footnote-43). Так на территории КНР существует государственный запрет на использовании в органах власти программного обеспечения и средств материально технического обеспечения зарубежного производства. Более того на территории страны находятся под запретом большинство распространенных во всем Мире информационных платформ, таких как Instagram. Facebook и т.д.

Осветив историю образования сети Интернет и зарубежного опыта, невозможно обойти стороной становление российского сегмента Интернета. Русскоязычная часть всемирной сети Интернет – Рунет (читается: [рунэ́т]) принадлежит к национальным доменным адресам «.ru», «.su» и «.рф». Ключевым в зарождении российского сегмента интернета является период с 1987 по 1994 год[[44]](#footnote-44). 28 августа 1990 года произошло слияние профессиональной научной сети, разработанной в Институте атомной энергии им И.В. Курчатова[[45]](#footnote-45), совместно с Министерством автомобильной промышленности с всемирной сетью Интернет, так началось существование российских коммуникационных сетей. 19 сентября 1990 года домен первого уровня «.su» прошел регистрацию в базе данных Международного информационного центра InterNIC, именно эта дата является днем подключения Советского Союза Социалистических Республик к всемирной сети Интернет. 7 апреля 1994 года в InterNIC прошел регистрацию первый российский домен «.ru».

Стоит отметить, что в всемирной системе Интернет преобладает английский язык. Более 51% информации представленной в открытом доступе именно на английском языке, однако эта доля имеет тенденцию к постепенному сокращению. Так, анализируя результаты исследования, проведенные компанией «W3Techs», с 2011 по 2017 год, доля английского языка на
веб-страницах Интернета сократилась с 58% до 51%. Разумеется, английский язык обладает статусом наиболее использующегося на планете, на нем говорят более 1.5 миллиардов людей. А в книге Д.Кристала английский язык и вовсе, впервые называется – глобальным языком. Но подобные аспекты лишь увеличивают значимость, что вторым по использованию в Интернете языком является – русский, да лишь 6,8% составляет его доля от всех существующих объемов информации в глобальной сети, но даже этот показатель опережает немецкий, испанский, французский и итальянский. Сохранение и преумножения информационного контента на русском языке является важным процессом, который необходимо всячески поддерживать и не останавливать. За последние десять лет русские пользователи заняли второе место по показателям прироста уникальных пользователей в сети Интернет (1825,8%)[[46]](#footnote-46).

Тенденция к накоплению и преумножению значимости информационных технологий в мировой политике, осознается многими государствами. Те страны, которые обладают передовыми информационно-коммуникационными технологиями, обладают возможностью увеличивать или сохранять существующий разрыв в информатизации от других стран. Исходя из этой информации некоторые страны, такие как США[[47]](#footnote-47) законодательно закрепили в нормативно-правовых документах, таких как доктрины и стратегии безопасности возможности ведения информационной войны[[48]](#footnote-48). Кроме того, США и ряд их союзников из НАТО оказывают серьезное противодействие против создания международной единой системы информационной безопасности под эгидой ООН, поскольку подобные глобальные системы обеспечения информационной безопасности значительно повлияют на лидирующее положение США и их союзников в области информационного глобального лидерства[[49]](#footnote-49).

Другие государства видят в такой ситуации потенциальную угрозу своим национальным интересам, и возможную уязвимость при информационной агрессии со стороны других стран[[50]](#footnote-50), исходя из этих фактов, государства ведут научные разработки в области информационного противоборства. Опыт вооруженных конфликтов и локальных воин последних десятилетий, наглядно демонстрирует эффективность применения методов информационного воздействия.
В Интернете, в отличие от привычных традиционных медиа-ресурсов находят свою аудиторию не только профессиональные журналисты, а любые участники информационного обмена. Последние благодаря сети Интернет наделяются возможностью осуществлять влияние на мнение, оценки и поведение многочисленной интернет-аудитории.

Подводя выводы к первой главе, автор констатирует, что проблемы и угрозы для безопасности государства исходящие из информационной сферы это реальность, с которой сталкиваются все страны в мире. Обширное и стремительное развитие технологий, открывший доступ к глобальному информационному обмену, практически в любой точке мира – явление новое и до сих пор не до конца изученное, исходя из этого, стоит крайне внимательно исследовать возможные последствия, вызванные информационным воздействием на общество. Государства, обладающие технологическим превосходством, используют его для преобразования в ощутимые политические выгоды для реализации своих национальных интересов, с использованием информационной сферы, как сферы влияния. Процесс глобального информационного взаимодействия, в который каждый день включаются миллионы новых субъектов, идет по пути создания единого информационного пространства для всего населения планеты. Критически важно, не допустить осуществления контроля или использования в своих целях данного пространства одним государством или частной компанией. Осуществление регулирования и управления информационной системой подобного уровня возможно исключительно консолидируемыми усилиями компетентных надгосударственных международных объединений.

Новые социальные процессы, возникающие в результате возникновения новых информационных технологий, меняют социальные механизмы взаимодействия внутри общества. У людей появляются новые источники информации, меняется характер общественных связей. Подвергаются изменениям устоявшиеся критерии оценки общества по уровню его развития. Создаются источники информации доступные каждому человеку на планете. Результатом продолжения развития современных технологий при сохранении его темпа будет являться дальнейшее совершенствование информационного взаимодействия всех структур каждого из вовлеченного в информационный обмен государств. Но, несмотря на наличие концепций высокого уровня теоретико-методологической проработки, автор данного исследования отмечает, что существует много неисследованных аспектов информационного взаимодействия. Существующие концепции рассматривают в основном индустриально развитые страны мира и их вовлеченность в глобальный информационный обмен (Японию, США, Германию и т.д)[[51]](#footnote-51), оставляя без должного изучения проблематику расслоения по технологическому развитию государств участников мирового информационного взаимодействия. Страны Африки, центральной Азии, и другие технологически «отстающие» регионы мира создают прецедент разделения по уровню вовлеченности в информационный обмен, который может стать угрозой устойчивому развитию в ближайшем будущем. В Российской Федерации, также складывается ситуация, констатирующая своим наличием значительный цифровой разрыв между крупными развитыми городами и регионами, несмотря на то что количество уникальных пользователей в России составляет – 109 миллионов при официальной статистике населения в 146 миллионов.

**Глава вторая**

**Политическая коммуникация в сети Интернет, правовое обоснование обеспечения информационной безопасности Российской Федерации.**

**2.1 Интернет как средство политической коммуникации.**

На сегодняшний день всемирная сеть Интернет выступает самостоятельным пространством для политической коммуникации. Проникновение современных информационных технологий в политику – является сложным, противоречивым и многоуровневым процессом. Сопутствующие данному, второстепенные процессы, протекающие в информационном пространстве, касающемся политических механизмов в стране: медаитизация и информатизация политики, использование сети Интернет, как средства для политической коммуникации и реализации политических технологий[[52]](#footnote-52). Дадим определение коммуникационному пространству. Коммуникационное пространство – это целостная среда, являющаяся разновидностью информационного пространства, в рамках которой осуществляется взаимодействие информационно-коммуникационного типа, между социальными субъектами, с использованием различных средств и техник коммуникационного взаимодействия.

Коммуникационное пространство, не смотря на наличие различных трактовок и толкований, без сомнений является одним из ключевых инструментов реализации как внешней, так и внутренней политики государства. Данный процесс имеет все предпосылки для продолжения в будущем и наращиванию темпов своего развития. Роли информационных коммуникаций и сети Интернет в частности будут только возрастать. Не стоит исключать возможность, что всемирная информационная сеть в ближайшем будущем станет ведущим источником политической коммуникации, тем самым смещая привычные традиционные СМИ[[53]](#footnote-53). Одной из основных причин, позволяющих утверждать это, является принцип, по которому осуществляется процесс коммуникации. В информационной среде, транслируемой в глобальной сети
Интернет, процесс взаимодействия происходит по принципу «от всех ко всем», то есть любой участник информационного обмена может получать, создавать, хранить и распространять информацию[[54]](#footnote-54). Набор критической массы аудитории происходит исключительно, по признаку соответствия предоставляемой источником информации спросу на информацию подобного характера и направленности. Потребление информации в сети Интернет не разрозненно, а системно, причем системы потребителей информации имеют ярко выраженные горизонтальные коммуникационные связи, говоря другими словами: пользователи, получая информацию обмениваются ей, становясь производителями собственной информации, на основе полученной или ретрансляторами исходной информации.

Важным аспектом является факторы притяжения систем потребителей информации. Такими являются: демографические, языковые, религиозные, профессиональные, политические или иные. В рамках системных сообществ в информационно-коммуникационной среде все участники данных систем обладают большим количеством горизонтальных связей и осуществляют регулярное информационно-коммуникационное воздействие друг с другом на основе данных связей.

Теоретик информационного общества Ё.Масуда, выдвинул гипотезу, согласно которой в современном обществе традиционные классы заменяются информационными стратами не имеющими социальной дифференциации.

Свободное обращение информации и мгновенная скорость её передачи способствует формированию гражданского общества, форсируют публичность и открытость политических процессов. Большой объем генерируемой, хранимой и передаваемой информации, вкупе со скоростью ей распространения увеличивают интенсивность её воздействия на аудиторию. Так же сетевые технологии дают обширное подспорье для социального контроля и социального вмешательства. Огромное количество источников информации не позволяет монополизировать информационный поток, более того, если получателям информации, её характер или содержание кажется сомнительным или негативным, сеть Интернет позволяет в этот же момент создать свой «комментарий», то есть сгенерировать новую информацию на основе полученной, которая вместе с главной теперь будет достигать всех получателей. Именно это отличие от традиционных СМИ, где процесс информационного воздействия происходит по принципу «от одного ко всем», то есть информационного монолога, заставляет говорить, о том, что процесс коммуникаций во всех сферах, особенно в политической вскоре в своем большинстве будет происходить на пространстве всемирной сети. Именно принцип распределения информации «от всех ко всем», создает уникальный прецедент для политической коммуникации, поскольку позволяет вступать в информационный обмен между властью и обществом без задержек по времени. Сбор информации, составляющей обратную связь на политические решения местного уровня или же реакцию социальных групп на реализуемый курс государственной политики, является важнейшим элементов политической коммуникации внутренней направленности. Стоит отметить так же влияние информационных технологий на механизмы становления власти в государстве. На сегодняшний день одержать победу на выборах, не имея доступа к традиционным средствам массовой информации считается невозможным, но с каждым годом, особенно в странах с высоким уровнем информатизации, отмечается опыт оказания влияния на политические предпочтения электората через сеть Интернет. В отличии от традиционных средств воздействия, этот обладает рядом существенных преимуществ. Среди них: мгновенность публикуемой информации, высочайшая скорость распространения, фактическая бесплатность, в отличии от ощутимых затрат на печать в СМИ, покупки физических рекламных мест и создания печатных материалов. Также в перечень преимуществ можно отнести отсутствие перед информацией, передающейся через глобальную сеть пространственно-временных границ и конечно огромный инструментарий мониторинга ситуации и реакции общественности на представленную информацию. Резюмируя озвученные тезисы, автор делает вывод, что в роль сети Интернет в политической коммуникации возрастает с каждым днем, из-за невозможности охвата всей информации, генерируемой в глобальной информационной сфере, к политической коммуникации можно отнести практически любую информацию в своем контексте, затрагивающую информацию, связанную с государством. Повышенное внимание также уделяется тем проблемам, которые затрагивают социальные опросы, изучение общественного мнения и голосованиям с использованием Интернет технологий. Пионерами в данной области выступили зарубежные коллеги из Федеральной программы содействия выборам (Federal Voting Assistance Program), при реализации которой, в ходе голосования проходившего в ноябре 2000 г. 84 избирателя отдали свой голос дистанционно, в режиме on-line, находясь на момент проведения выборов за границей. То есть сеть Интернет не только предоставляет кандидатам возможность для информирования электората о целях и задачах своего выдвижения, создавая возможность для мгновенной обратной связи и консолидации вокруг существующих проблем в социуме, но и позволяет любому гражданину проявить свою гражданскую позицию вне зависимости от его текущего местонахождения.

С.В. Володенков в своей научной работе «Особенности интернета как современного пространства для политических коммуникаций», указывает что: «Интернет, выступая изначально в качестве средства коммуникации общей направленности, со временем своей эволюции превратился в пространство для политических коммуникаций, выступающее онтологической основой для формирования виртуальной реальности, отличной от сформированной традиционной медиареальности, описанной в большинстве существующих научных исследований»

Производство, хранение и распространение информации становятся основным фактором политической коммуникации. Зарождаются и получают динамический скачек развития сложные информационные технологии, основные принципы социальной стратификации меняются, роль организации и управления информационным обменом доминируют в обществе.

Процесс манипулирования массовым сознанием, возможности для которого с развитием информационных технологий расширяются в геометрической прогрессии занимает одну из важнейших ролей в XX веке. Новые средства информационно-коммуникационной передачи информации и их скорость позволяют охватить пропагандой миллионы людей в самое короткое время.[[55]](#footnote-55) Подобное получение информации, особенно о предмете, в котором конечный адресат не компетентен (социально-политические события регионального, государственного и мирового масштаба), позволяет получать образы и модифицировать объективность восприятия действительности путем ментальных представлений, основой для которых является только та часть освещения объекта, которую представил источник и производитель информации (Интернет – СМИ). В условиях нарастающей информатизации и развития технологий, человек постоянно нуждается в своевременном освещении актуальных тем. Причем чем больше информационных «маркеров» на карте информационной картины дня, тем меньше фактор «удержания внимания» на конкретной тематике[[56]](#footnote-56). Иными словами, информационные технологии совершили скачек, опережающий развитие человеческих способностей. Мировое общество стало генерировать такое количество информации, которое невозможно воспринять полностью. В общем информационном «шуме» человек старается найти и обработать именно ту информацию, которая интересна, ведь неразрывная информационная связь с окружающей индивидуума действительностью – является важнейшим условием нормального жизнедеятельного цикла современного человека. Но объем окружающей информации оказывает огромное давление на адресата. Помимо действительно качественной и необходимой, существуют десятки видов «вредной», а зачастую и «пустой» информации, к которой относится все виды маркетинговой, рекламной, заведомо ложной, недостоверной и некомпетентной информации.

В современной науке ещё не сложилось единой общепризнанной концепции манипулирования сознанием. Это указывает на то, что теоретические исследования по данной проблеме находятся на стадии разработки[[57]](#footnote-57). Однако, интенсивность манипулятивного воздействия на сознание возрастает, затрагивая все сферы жизнедеятельности общества. Манипулирование сознанием перерастает в особый вид деятельности и превращается в социальную проблему, угрожающую как политической, так и другим видам коммуникации. Существует несколько приёмов манипуляции в сети Интернет.

1. Искажение информации. Ввиду огромного количества источников информации и ретрансляторов, обычному пользователю зачастую очень трудно отличить правду от искусно созданной фикции.
2. Принцип шумового воздействия. Если есть необходимость «заглушить», лишить аудитории источник информации, при наличии материально технических ресурсов и отработанных механизмов, его можно «утопить» в хаотическом потоке бессмысленной информации, генерируемой в бесконечном количестве[[58]](#footnote-58).
3. Решение проблем путем дробления. Если существует наличие проблемы, которая не должна быть подвержена социальной огласке или обсуждению, применяется принцип дробления проблемы на составляющие части. Деление основной информации на фрагменты возможно только до её предания информационной огласки и происходит таким образом,
что в дальнейшем потребители данной информации не могли увязать взаимосвязь между двумя отдельными фрагментами в одно целое. Сопровождается такой приём постоянным обновлением информации по освещаемой проблематике, в таких условиях рядовой потребитель информации, без специальной подготовки и компетенции, просто не в состоянии осмыслить и понять до конца заранее сфабрикованные информационные блоки.
4. Использование эстетической информации. По своей природе, человек получая семантическую информацию склонен действовать согласно сложившимся у него внутренним убеждениями и нравственным ограничителям. Но используя различные технологические эффекты, манипуляторы снабжают потребителей информации эстетической информацией, в которой заключен смысл политизации информации, поскольку побуждение подобной информацией направлено не на процесс познания, а на внушение устойчивых символов, заранее прописанных в контексте предоставляемой информации.

Подводя итоги анализа политической коммуникации в всемирной сети Интернет, автор обуславливает следующие последствия развития данного процесса.

Первое: в условиях становления и развития информационного общества можно указать на снижение стоимости обслуживания информационного обмена (создания, хранения и распространения информации), результатом данного условия является увеличение количества людей, наделенных возможность оказывать информационное воздействие на широкий круг лиц. То есть формируются акторы политической коммуникации нового типа. Создаются предпосылки для уменьшения неравенства в реализации политических прав граждан. Все большая реализация гражданами своих политических прав и свобод, выражение своего сформированного мнения, увеличивает оказываемое социальное давление через информационную сеть на деятельность государства.

**2.2 Система обеспечения информационной безопасности Российской Федерации**

«Правительство Российской Федерации реализует направления по обеспечению информационной безопасности страны: разрабатывает целевые программы и выделяет необходимые средства из бюджета, координирует деятельность федеральных органов власти и органов исполнительной власти субъектов, осуществляет меры по предотвращению возможных угроз информационной безопасности, издает постановления и распоряжения в области обеспечения информационной безопасности». Совет Безопасности РФ проводит работу по выявлению и оценке угроз информационной безопасности Российской Федерации.

Совет Федерации, подготавливает проекты решений по предотвращению угроз и разрабатывает предложения по обеспечению информационной безопасности, а так же предложения по дополнению или же уточнению положений принятой Доктрины информационной безопасности РФ. Федеральные органы исполнительной власти обеспечивают исполнение нормативно-правовых документов, приказов Президента РФ в сфере информационной безопасности. В состав Федеральных органов исполнительной власти входят следующие государственные органы, ведомства: ФСБ[[59]](#footnote-59) России, ФСО России, МВД России[[60]](#footnote-60), Роскомнадзор и Минкомсвязи России[[61]](#footnote-61). Статья 11.2 Федерального Закона «О Федеральной службе безопасности» обеспечение информационной безопасности – деятельность органов федеральной службы безопасности, осуществляемая ими в пределах своих полномочии при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе и использованием инженерно – технических и криптографических средств.

Основными задачами ФСБ России по обеспечению общей и информационной безопасности являются:

• Организация выявления, предупреждения и пресечения разведывательной и иной деятельности специальных служб иностранных государств и отдельных лиц, направленной на нанесение ущерба безопасности Российской Федерации.

• Обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям осуществляющим техническую разведку.

• Формирование и реализацию в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности.

• Организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за пределами территории Российской Федерации.

Федеральный закон от 27.05.1996 №57 « О государственной охране» Федеральная служба охраны (ФСО)[[62]](#footnote-62) России осуществляет нормативно-правовое регулирование, контроль и надзор в сфере президентской, правительственной и иных видов специальной связи и информации, предоставляемой федеральным органам государственной власти субъектов РФ и другим государственным органам.

 Основными задачами ФСО России являются:

• Организация и обеспечение безопасности специальной связи и информации, предоставляемой государственным органам.

• Осуществление государственной политики в области информатизации Российской Федерации и координация работ, в данной сфере.

• Разработка и реализация мер по обеспечению информационной безопасности Российской Федерации.

В рамках определенных Положением о Министерстве обороны Российской Федерации, Министерство обороны Российской Федерации выполняет следующие функции по обеспечению информационной безопасности:

• Организует и курирует деятельность по обеспечению информационной безопасности в Вооруженных Силах Российской Федерации.

• Осуществляет разведывательную деятельность по обеспечению информационной безопасности и предотвращению возможных реальных и теоретических угроз.

• Устанавливает нормативно-правовыми актами и другими документами нормативного характера требования к техническому регулированию оснащения используемому в Вооруженных Силах Российской Федерации, в целях защиты сведений составляющих государственную тайну.

Указ Президента РФ от 19.07.2003 №927 «Вопросы Министерства внутренних дел Российской Федерации» . Министерство внутренних дел Российской Федерации в пределах своих полномочий обеспечивает:

• Защиту прав и свобод граждан в информационной сфере.

• Предупреждение, выявление, пресечение, раскрытие и расследование преступлений совершенных в информационной сфере и с применением современных технологий.

• Защиту сведений составляющих государственную и иную охраняемую законом тайну.

Министерство связи и массовых коммуникаций Российской Федерации в целях обеспечения информационной безопасности выдвигает следующие требования.

• Требования к средствам и техническим оснащениям информационного обмена для проведения оперативно-розыскных мероприятий по согласованию с уполномоченными государственными органами.

• Требования по информационной безопасности информационных систем, в том числе информационных систем персональных данных, информационно-телекоммуникационных сетей и других сетей связи.

Постановление Правительства РФ от 16.03.2009 №228 «О федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» Роскомнадзор осуществляет следующие полномочия в системе обеспечения информационной безопасности Российской Федерации:

• Выполняет государственный контроль в информационной сфере за соответствием персональных данных законодательству Российской Федерации в области персональных данных.

• Осуществляет государственный контроль и надзор в сфере информационных технологий, в сфере защиты детей от информации, причиняющей вред их здоровью и развитию.

• Обеспечивает формирование и создание единой автоматизированной системы «Единый реестр доменных имен, указателей страниц сайтов в сети Интернет и сетевых адресов, позволяющих идентифицировать сайты в сети Интернет, содержащие информацию, внесенную в список запрещенной информации в Российской Федерации»

• Ведет реестр операторов, осуществляющих обработку персональных данных.

**2.3 Применяемая нормативно-правовая база.**

Говоря о Российской Федерации, информационная сфера является наиболее уязвимым компонентом системы национальной безопасности государства. Поскольку преимущество над многими, практически над всеми странами по уровню развития современных систем традиционного и новейшего вооружения уже не является предметом споров. Но область информационно-коммуникационных технологий, а также связанных с ними информационных областей осуществления государственной внешней и внутренней политики по-прежнему нуждаются в развитии и финансировании. Особенно в условиях формирования единого, глобального информационного пространства, где жизнедеятельность общества определяется уровнем развития, безопасностью, а также непрерывным функционированием информационной среды.

В виду вышеизложенного автор считает необходимым обосновать нормативно-правовую составляющую системы обеспечения информационной безопасности в Российской Федерации.

Обеспечение информационной безопасности является деятельностью по недопущению реализации угроз на важные интересы личности, общества и государств. Предотвращение опасностей и обеспечение необходимого уровня безопасности информационной сферы. Описанная деятельность осуществляет ликвидацию не только угроз информационной безопасности, но и источников подобных угроз[[63]](#footnote-63). Система обеспечения информационной безопасности – это совокупность сил и средств обеспечения информационной безопасности. Федеральные целевые программы определяют бюджетные источники финансирования выделяемые на реализацию мер противодействия угрозам информационной безопасности. Средства технического обеспечения – являются совокупностью технических и программных средств обработки и защиты информации. В состав данных средств включены методические обеспечения использования технических средств защиты информации. Методические обеспечения – это организационно-технические нормы, разработанные в целях обеспечения безопасности информационной инфраструктуры. Государственная политика Российской Федерации в области информационной безопасности, возможна только при согласованных действиях всех элементов системы обеспечения информационной безопасности.

Комплексные проблемы обеспечения информационной безопасности страны, рассматриваются на заседания Совета Безопасности РФ, Государственного совета РФ, Общественной палаты РФ, совещаний Министерства обороны РФ, а также иных совещательных и консультативных органов.

Президент Российской Федерации, в посланиях Федеральному Собранию каждый год обозначает приоритетные направления государственной политики, в том числе, в области обеспечения информационной безопасности.

Для своевременного и полного обеспечения информационной безопасности Российской Федерации, необходимо формирования структур способных по своей структуре и компетенции оказывать противодействие информационно-психологическому влиянию. Задачей данных структур является противодействие информационной угрозе, обеспечение информационно-психологической безопасности личности и информационной безопасности общества и государства. Осуществление мер по нейтрализации информационных операций, на местном, региональном и федеральном уровне[[64]](#footnote-64). Деятельность подобного характера активно стала проводится только в 1990-х годах, когда Российская Федерации столкнулась с перечнем реальных угроз в информационной сфере, решение которых, существовавшими методами, оказалось невозможным[[65]](#footnote-65). Особое влияние на формирование структуры информационной безопасности нового типа, оказал фактор существенного технологического отставания Российской Федерации от своих геополитических соперников, которые используя преимущество в технологиях и средствах информационного воздействия, проводили информационную экспансию в политической, общественной, экономической и культурной области. Единственным возможным ответом на проявления агрессии в информационной сфере явилась новая стратегия развития Российской Федерации, лоббируемая главами правительства Е.Примаковым, С.Степашиным и наконец В. Путиным. Концепция новой стратегии заключалась в формировании государственной системы нового типа, сильного, крепкого, способного выдержать все вызовы быстроменяющегося мироустройства. В рамках данной концепции был разработан и принят ряд основополагающих документов, регулирующих, в том числе все направления обеспечения информационной безопасности и осуществления информационной политики Российской Федерации. Данные документы составляют правовое обоснования обеспечения информационной безопасности государства и являются основными нормативно-правовыми документами, регламентирующими деятельность структур и ведомств Российской Федерации, в комплекс задач, которых входит обеспечение достаточного уровня информационной безопасности страны.

1. «Концепция государственной информационной политики Российской Федерации» Концепция была разработана в 1998 г, Комитет информационной политики и связи Государственной Думы Федерального Собрания одобрил данный документ 21 декабря 1998г. В принятой концепции были закреплены следующие принципы государственного регулирования информационной сферы.

- Принцип открытости: Все события и элементы информационной политики государства, открыты для обсуждения обществом. Мнение, выраженное большинством - является критичным для государства и должно быть учтено в принятии решений.

- Принцип равенства интересов: Политический Процесс в Российской Федерации должен учитывать интересы всех участников информационной деятельности, не делая исключений по принадлежности к слоям населения или положению в обществе.

- Принцип системности: При принятии и реализации политических решений, руководством страны должны учитываться максимально полные последствия и все субъекты, затрагиваемые решением.

- Принцип социальной ориентации: Основной направленностью государственной информационной политики должны быть: обеспечение социальных интересов общества.

Проводя анализ «Концепции государственной информационной политики Российской Федерации», можно заметить, что российское руководство выбрало курс на централизацию государственной политики в информационной сфере, что позволяет решить проблемы, относящиеся к внешним проблемам обеспечения информационной безопасности.

Во-первых, это контроль информационных потоков внутри информационной сферы Российской Федерации и объединенных информационных сфер со странами союзниками, а следовательно
не допущение потери контроля над данными потоками информации в пользу геополитических противников. Во-вторых, прослеживается стратегия направленная на увеличение российского информационного присутствия обеспеченного достоверной и открытой информацией в источниках информации других государств.

1. «Концепция формирования информационного общества в Российской Федерации» Одобрена Государственной комиссией по информатизации при Государственном комитете Российской Федерации по связям и информатизации 28 мая 1999 г.

В данной концепции наиболее полно описаны основные этапы перехода Российской Федерации к информационному обществу, возможные информационные угрозы при данном переходе, а также основные направления деятельности государственных структур при реализации данной концепции. Особый интерес представляют положения, описывающие роль российского государства в переходном процессе[[66]](#footnote-66). Важнейшей составляющей подобного перехода является принятия участия нашим государством процесса формирования международного информационного обмена[[67]](#footnote-67).

Обе вышеуказанные концепции направлены на взаимодействие с другими государствами, обмен технологиями и участие в международном процессе обеспечения глобальной информационной безопасности. Подобное участие Российской Федерации в международных инициативах, является важной частью государственной политики, поэтому обе принятые концепции – обязательны для исполнения.

1. «Доктрина информационной безопасности», утвержденная в 2000 г., утратившая силу в настоящее время, в силу утверждения Президентом РФ новой доктрины 06 декабря 2016 г.

В документе указывается, что специальные службы разных государств используют технические средства информационного воздействия, с целью дестабилизации внутриполитической ситуации в Российской Федерации. А в отдаленных регионах мира, подобные манипуляции уже привели к разрушению суверенитета и нарушению территориальной целостности государств. Отмечается, что к подобной деятельности привлекаются религиозные и этнические организации. Подобные действия, с использованием информационного воздействия в глобальной информационной сфере направлены на создание социальной напряженности. Отмечается что российские СМИ подвергаются дискриминации, российским журналистам чинят препятствия в их профессиональной деятельности. В разряд особых угроз выведено информационное воздействие на население Российской Федерации, в первую очередь на молодежь. Происходит манипуляция общественным мнением, замена культурных устоев, размывание традиционных российских духовных ценностей.

Доктрина информационной безопасности Российской Федерации, провозглашает одной из частей информационной политики: уменьшение уровня зависимости отечественных информационных сетей от зарубежных информационных технологий. «Состояние информационной безопасности в экономической сфере, характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказании услуг[[68]](#footnote-68)»

Стоит отметить, что современные аспекты информационной безопасности, ими стали технологии, которые, которые будут внедрены в будущем в нашей стране, в доктрине они описаны как «изначально устойчивые к различным видам воздействия»

В Доктрине информационной безопасности закреплены основные интересы национальной безопасности страны в информационной сфере. В рамках данной исследовательской работы, можно выделить три основных направления.

Первое: Необходимость соблюдения и обеспечения достаточного уровня информационной безопасности конституционных прав и свобод граждан при получении, хранении и использовании информации. Отмечается важность хранения и укрепления традиций и ценностей нашего общества, укреплении патриотизма среди населения, формирования здравой политической позиции, основанной в первую очередь на достоверных и компетентных источниках информации.

Второе: Средства технического обеспечения имеют огромное значение на возможность обеспечивать достаточный уровень информационной безопасности, как от внешних, так и от внутренних угроз. По данной причине перед Российской Федерацией стоит задача по развитию новых информационно-коммуникационных технологий и технических средств обеспечения глобального информационного обмена, а также по увеличению производственных и трудовых мощностей в информационной сфере, выполнение данных задач, сделает возможным не только полное обеспечение внутреннего рынка средствами информатизации и телекоммуникации, но и выход на международный рынок.

Третье: Информационное обеспечение государственной политики в области обеспечения информационной безопасности Российской Федерации должно подкрепляться достоверной и открытой информацией, доводимой до сведения российской и мировой общественности открыто и без искажений. Данная информация должна освещать позицию Российской Федерации по социально значимым вопросам.

Несмотря на логическую обоснованность подобных задач, необходимо понимать, что данная составляющая информационной безопасности страны, включает в себя обеспечение процесса обработки информации, то есть её накопления, создание, хранения и эффективного использования, в условиях наличия угроз её безопасности.

1. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». Утверждены Президентом Российской Федерации 24 июля 2013 г. № Пр-1753

В настоящем документе определяются основные угрозы в области международной информационной безопасности, цель и задачи государственной политики Российской Федерации в области международной информационной безопасности. «Интенсивное развитие информационных и коммуникационных технологий, их широкое применение во всех сферах деятельности человека создали условия для формирования глобальной информационной инфраструктуры, которая предоставила качественно новые возможности социализации людей, их общения и доступа к накопленным человечеством знаниям. В современном обществе информационные и коммуникационные технологии являются основным фактором, определяющим уровень социально-экономического развития и состояние национальной безопасности. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года призваны способствовать активизации внешней политики Российской Федерации на пути достижения согласия и учета взаимных интересов в процессе интернационализации глобального информационного пространства.»

**2.4 Информационное воздействие как угроза социальному благополучию общества**

Любое государство на планете в настоящее время находится внутри глобальных информационных потоков и является частью информационного обмене в масштабах всей планеты. Не смотря на возможные внутренние ресурсы по ограничению и фильтрации информации, которые присутствуют в таких государствах как Китай, невозможно контролировать информационные потоки за пределами собственной «внутренней сети». Изучая вопрос негативности информационного воздействия и его разновидностей, автором данного исследования было отмечена недостаточность изученности и освещенности данной проблематики в трудах отечественных ученых. Основная направленность научных изысканий наших соотечественников сфокусированы непосредственно на информационной безопасности и аспектах её обеспечения. В иностранной литературе, наоборот технологии как индивидуальной, так и групповой защиты разработаны весьма полно. Существует даже профессия, формированию которой, общество полностью обязано стремительному развитию технологий – специалист устранения негативных последствий информационного воздействия. Подобная практика пока существует только в зарубежных странах. Возвращаясь к научным изысканиям внутри Российской Федерации, можно отметить труды Смирнова А.И[[69]](#footnote-69) и Россошанского А.В[[70]](#footnote-70), направленные на систематизацию и разработку методов и приёмов защиты от информационного воздействия. Но устойчивые начальные модели общественного строя, иначе говоря «социальные системы», которые подвергаются анализу в научных исследованиях и даже в нормативно-правовых актах (Доктрина информационной безопасности), являются по своему существу исходно – «нормальными» или «стабильными социальными системами», не имеющими ярко выраженных недостатков или дефектов. Автором данного исследования отмечается, что Российское общество, вступившее в глобальный информационный обмен, а, следовательно, вставшее на путь становления «цифровым обществом» изначально по своей исторически сложившейся модели не может быть отнесено к «стабильным», поскольку социальная система нашего государства была образована в результате разрушения и дробления более крупной системы, при прекращении существования СССР. Причиной подобных изменений стало именно поражение в информационном противоборстве, в котором столкнулись две общественные модели, два мировоззрения. С.Расторгуев в своих исследованиях подробно описывал причины и признаки почему Советский Союз не смог одержать победу в информационной войне. Следовательно, возвращаясь к первоначальному тезису, социальная система, сформированная при деформации прошлой, устоявшейся системы, разделившаяся на несколько закрытых и не связанных друг с другом систем по территориальному и теперь уже государственному признаку не может быть «стабильной», соответственно, проводить научные изыскания с целью установления механизмов по противодействию информационному воздействию необходимо беря за основу «особый тип социальной системы». В системе описанного типа подсистемы на начальном этапе своего существования (1993-1996 г.) поражены и не способны функционировать и выполнять процесс принятия решений. Подобное состояние подсистем, дает возможность как внешним, так и внутренним заинтересованным в дестабилизации систем акторам совершать действия манипулятивного характера или даже прямые акты манипуляции, направленные на подмену или замещение целей, выполняемых подсистемами, изменения оптимальных путей взаимодействия подсистем между друг другом, а также механизмы, вызывающие дисфункцию как подсистем, так и всей системы в целом. Органы управления, являющиеся как частью системы, так и подсистем, в зависимости от своей значимости и охватываемой области принятия решений, а также сформированного внутреннего ресурса, в ситуации деструкции общей системы, теряют объективную возможность различения «своей» информации от «чужой». Для преодоления данной ситуации необходима разработка моделей, включающих в себя механизм подобного различения. Объективно операторами подобных моделей выступают субъекты информационного обмена, в ходе которого ими осуществляется «освоение» объектов информационного обмена, а следовательно и фильтрация их по содержанию, области генерации и направленности.

Помимо фильтрации и освоения объектов информационного обмена, поступающих из внешних источников, остро стоит необходимость мониторинга социальных отклонений в информационном обмене генерируемом и хранящемся «внутри» информационного поля страны. Володенков С.В. в своей научной работе[[71]](#footnote-71) отмечает, что Интернет, при своем наборе определенных угроз и отрицательных сторон, обладает объективно положительной чертой, заключающейся в возможности обеспечения обратной связи для всех институтов гражданского общества. Именно по этой причине необходимо поддерживать проявление общественного мнения и гражданской позиции среди всех слоев населения. Скорость передачи информации, её поиска, неограниченное время хранения и сравнительно не дорогая стоимость использования ставит информационный обмен между гражданами и органами власти в информационной сети Интернет на первое место по удобности, простоте, скорости и объективности. На данный момент остро стоит ряд проблем в данной области: На осуществление субъектами подобной деятельности необходимо постоянное материально-техническое обеспечение, помимо этого нужно обеспечить рост уровня деятельности социальных и государственных субъектов, которые будут осуществлять функции обратной связи различного рода. В данном контексте так же важно направить деятельность на учреждение новых и развитие старых институтов самоуправления, поскольку именно подобные институты являются «двигателями прогресса» в общественном сознании.

В ходе существования систем и зависимых от них подсистем в информационном обмене, цели, которые формируют субъекты данного обмена могут различаться. В зависимости от целей и задач, которые стоят перед субъектами. К примеру, они могут иметь конструктивный характер – развитие и достижение новых состояний развития, которые ведут к улучшению качества функционирования системы, а следовательно, и подсистем или же напротив целью может быть генерирование состояния разрушения структуры и системы и функций, которые она выполняет, тогда это повлечет за собой понижения эффективности деятельности системы и её качества функционирования соответственно. Но в обоих случаях действия, осуществляемые в информационном поле – являются информационным воздействием, осуществляемым с помощью поступающей на вход информации, она может являться как полезной, так и бесполезной. Причем стоит отметить, что информационная составляющая, которая оказалась не применимой или не содержательной для одного из элементов системы не обязательно будет так же не применимой для иных элементов той же системы, поскольку подсистемы и субъекты общего информационного обмена обладают различными компетенциями, уровнями доступа к информации, а также отличающимися возможностями по передачи информации дальнейшим адресатам, а следовательно разным уровнем «информационного доверия».
Ценность осуществляемого информационного воздействия возможно установить, если обладать точными данными о целях субъекта обмена в отношении управляемого объекта. Стоит отметить что, беря во внимание невозможность охвата и анализа всей существующей и возникающей информации, следовательно, ценность информационного воздействия невозможно оценить в кроткосрочной перспективе. Ценность, ровно, как и цели, поставленные перед информационным воздействием, всегда имеют «отложенный» характер. Причиной подобной особенности в характеристике информационного воздействия является особенность – «амбивалентность». Подобный феномен имеет определение, которое в контексте исследования необходимо озвучить. Амбивалентностью информационного воздействия является содержание в контексте всего объема информации или его некой части опасности для объекта управления. Например, абсолютно достоверная информация может нанести вред или даже быть губительной, поскольку эмоциональные взаимоотношения и ожидания у получателя информации достигли критической точки, говоря иначе полученная информация по критически важным вопросам может привести к разрушению подсистемы, по причине крайней заинтересованности в информации. Основываясь на этом, можно сделать вывод что бывают ситуации, при которых дезинформация системы может быть использована во благо. Но для более точного анализа и применения подобных механизмов важно иметь дееспособный механизм «освоения» субъектом информационного обмена получаемой информации, который был описан ранее.

Опираясь на вышеперечисленные факты и характеристики, становится ясно, что разработка и внедрения инструментов и эффективных мер обеспечения защиты от информационного влияния и осуществление процессов по нейтрализации уже оказанного влияния –является приоритетной задачей государственного масштаба. Социологические исследования, охватывающие разные слои и страты Российского общества, среди прочих, автор выделяет исследование О.Г. Павельева фиксирует не утешающую статистику: население Российской Федерации, теряет способность к критическому мышлению, что означает открытость общественного сознания для манипуляций и внешних воздействий. Помимо этого, отмечается повсеместное увеличение гипнабельности общества – показателя, состоящего из нескольких критериев оценки и восприятия информации у опрашиваемых, указывающий на уровень подверженности информационному воздействию. Показатели данных социологических исследований указывают на критическое сокращение основы, которая может осуществить процесс выхода из кризиса систем информационного обмена. Под «основой» понимается внутренний «слой» Российского общества, обеспечивающий не только целостность социального строя, но и его идентичность стране, её историко-культурной составляющей и являющийся ресурсом для обеспечения устойчивого существования путем проецирования сложившихся устоев норм и ценностей на будущее[[72]](#footnote-72).

Дополнительно стоит отметить, что в подобных условиях в современной России «перспектива будущего исчезает, а настоящее увековечивается». Решение, которое могло бы удовлетворить большинство и на которое, данное большинство уповает не может быть воспринято или сформулировано в сознании, поскольку информация появляется беспорядочно и непрерывно. Именно бесконечность потока информации в информационном поле и её объем является ключевой проблематикой к критическому восприятию среди широких общественных слоев. В ходе вступления нашего государства в глобальный информационный обмен, количество как информации, так и источников её происхождения будет увеличиваться буквально с каждым днем[[73]](#footnote-73). В подобных условиях в общественном сознании необходимость наличия сформированных моделей решения тех или иных задач, на которые источники власти могут отреагировать, используя механизм обратной связи, будет только расти. Формирование подобных категорий мышления очень важно, поскольку отображает обобщенность чувств и консолидацию общественных интересов[[74]](#footnote-74). Стремление поиска обобщенного, универсального и компромиссного решения не имеет единой цели или четко выраженного требования к конкретному органу, оно пронизывает все возможные проблемы и сложности, зарождающиеся в обществе. Государственная информационная политика, по мнению автора, должна разработать механизмы по включению описанного процесса в разряд приоритетных, поскольку именно стремление населения страны к решению проблем, диалог народа с органами власти и принятия решения, ведет к внутреннему сплочению внутри государства.

Формированию становления и укрепления устойчивого механизма противодействия информационному воздействию, способствует консолидация общественности вокруг устоявшихся в обществе устоев, традиций, культурных ценностей и объектов культурного наследия, нравов, бытовых аспектов и общественных идеи. Осуществить подобную консолидацию невозможно без привлечения к ней субъектов информационного обмена специальных категорий: деятелей культуры, научного сообщества, исследователей, писателей, специалистов историков, обществоведов, всех слоев интеллигенции, общественных движений, лиц с активной гражданской позицией и заинтересованных лиц и организаций. Формирование устойчивого информационного иммунитета (возможность быть не подвластным деструктивному информационному воздействию) должно происходить на основе централизации общественных идей и осуществляться на основе принципов: релевантности, субъективности и научности.

Значимость релевантности обосновывается целью социального конструирования, которая в первую очередь нацелена на будущие качественные улучшения общества. Следовательно, подобное конструирование должно обладать релевантным смыслом для всех слоев населения, то есть всех участников информационного обмена. Придерживаясь подобной логике необходимо формировать соответствующие формы коммуникаций, завершением которых будет являться построение систем. Несмотря на то что смысл – является понятием и явлением субъективным, но именно обобщенная идея наличия смысла в сознании широких слоев населения в процессе консолидации и объединения – выступает «структурой» или можно сказать «материалом», который выступает связующим для субъектов и соединяет их в систему[[75]](#footnote-75). Именно смысл и его четкое наличие становится основой для взаимодействия сторон любого масштаба. Перед государственной информационной политикой стоит задача по завязке формируемого в общественном сознании «смысла» с жизненно важными потребностями страны, в подобной «связке», это становится мотиватором с огромным потенциалом, который направляет общество на достижение социально значимых и полезных целей в условиях обобщенности и консолидации.

Принцип субъективности обозначает что субъект информационного обмена, подверженный информационному воздействию, то есть личность, индивидуум, человек, должен обладать основополагающим принципом – наличием воли. Субъект должен не только осознавать наличие информационного воздействия, уметь различать его направленность, источник и обладать желанием защитить себя в случае если воздействие расценивается как негативное, но и иметь в себе силы реализовать это желание. То есть обладать определенным уровнем социальной активности. Консолидацию и объединение общественно важных традиций и устоев необходимо осуществлять вокруг субъектов, которые являются устойчивыми к информационному воздействию, поскольку, являясь информационным центром системы определенного уровня, субъект информационного обмена должен быть устойчив к информационному воздействию, ведь он является источником информации для широкого круга лиц, а также объектом «кристализации» общественной идеи и смысла консолидации общества.

Научность централизации общественных идеи исходит из той роли, которую играет в разработке концепций информационной безопасности телеологический подход. Следовательно, помимо смысла, необходимость наличия которого описано выше, в механизме формирования устойчивого информационного иммунитета, необходимо наличие четкой и сформированной цели. В целях обоснования наличие цели, как решающего элемента системы консолидации общества, автор приводит цитату С.П. Расторгуева из научной работы «Философия информационной войны»: «Развал любой сложной информационной системы, будь то государство, предприятие, коллектив, может свидетельствовать об отсутствии у нее доминирующей цели. И наоборот создание порядка из хаоса объясняется наличием этой самой цели. Цель, ставшая доминирующей, сумевшая подчинить или уничтожить своих соперников, а тем самым стать истинной, спасает не только себя, но и всю систему в целом».

Если рассмотреть, как способ консолидации общества - политическое пространство, то в Российской Федерации необходимо признать отсутствие заданного вектора построения политических организаций. На май 2019 года , в России зарегистрировано более трех десятков различных политических партий, а объединений и движений еще больше. К глубокому сожалению подавляющее большинство из них не имеет цели и смысла объединения всех уровней системы. Они существуют по принципу верховенства личности над смыслом и целью. (ЛДПР,Яблоко и др.), другие же, коих не большинство существуют по принципу доминирования количественных характеристик направленных на расширение политической коньюнктуры и влияния. (Единая Россия), но, как и во всех процессах в угоду массовости, конечно поступаются значимостью цели и смысла, поскольку Российская Федерация является уникальным государством по количеству национальностей и охватываемых территорий, и применение унифицированных целей и смысловых векторов, не может функционировать верно. Подводя итог, автор подчеркивает что политическая интеграция субъектов информационного обмена, направленная на консолидацию и объединение общества, должна выйти за рамки определенных сфер жизни: экономики, общества, политики, науки или культуры и начать использовать

**Глава третья.**

**3.1 Обоснование основных направлений оптимизации обеспечения информационной безопасности в Российской Федерации.**

Эмпирический анализ существующих подходов к обеспечению информационной безопасности и рассмотрение реализуемых механизмов по предотвращению информационного воздействия
на субъекты информационного обмена не может являться завершенным или полноценным, поскольку он не доведен до конечной точки реализации анализа подобного типа – обоснованию конкретных направлений деятельности субъектов направленных на обеспечение данного вида безопасности. Автором данного исследования выделяется отдельное направление – политическое, анализ которого в свою очередь уже осуществлен в ряде политологических исследований.

В данной работе были использованы термины и понятия «информационная политика», «информационная безопасность личности или государства», «процесс информатизации», «политика в сфере информационной безопасности», но не было выявлено и установлено точных взаимосвязей между анализируемыми и раскрываемыми терминами и понятиями. Автор задается вопросом: корректно и правильно ли употребляют подобные определения, какова их взаимосвязь друг с другом? Корректно ли используются гигантские объемы информации, которые производит глобальное информационное общество[[76]](#footnote-76)? Эффективны ли меры, которые направлены на обеспечение информационной безопасности государства? Обеспечивают ли они решение реальных проблем в области информационной безопасности? Ряд западных государств, среди которых Соединенные Штаты Америки, страны Западной Европы и Япония за последние годы сформулировали и смогли обосновать ответы на подобные вопросы[[77]](#footnote-77): существует необходимость в создании особых условий, которые будут являться условиями, обеспечивающими устойчивый переход строя общества к информационному. Важнейшим условием для формирования для становления информационного общества является взаимосвязь между тремя компонентами: социально-структурными изменениями, которые неизбежно возникают при изменении общественного строя, информацией, которая является продуктом, а в некоторых аспектах и товаром и самим компонентом новых информационных технологий. Именно взаимодействие и взаимосвязь всех трех компонентов, на условиях их равной значимости обеспечит наиболее эффективный и плавный переход формации общества. Возвращаясь к окончательному обоснованию используемых понятий, автор обозначает информационную политику – как особый тип поведения людей и порождающийся в результате их поведения – механизм управления общественными процессами. Стоит отметить, что многообразие проявлений процесса «политики» не обозначает неопределенности её результатов и форм, сущность процесса обозначается через категорию «власть». Следовательно, политика информатизации является деятельностью по производству, анализу, хранению и использованию информации всеми субъектами информационного обмена, обуславливающему роль информации, как общественного ресурса[[78]](#footnote-78). Дополнительно предполагается внедрение технологий, которые обеспечат массовое использование методов по сбору передачи и хранения информации. Формулируя вывод из обозначенных тезисов, можно сказать, что основная цель при трансформации общества заключается в функционировании всех элементов и структур общества на основе информационных технологий. В ходе построения информационного общества, не только в Российской Федерации, но и в опыте других государств, была выявлена особенность подобной трансформации. Наиболее точно её описывает Боридьков И.С.[[79]](#footnote-79)
« построение социального действия и политики вокруг первичных идентичностей, либо прописанных, укоренившихся в истории и географии, либо построенных заново в поисках общих точек соприкосновения общества в области духовности и общих смыслов», «Первые исторические шаги информационных обществ характеризуются преобладанием идентичности как организационного принципа». В свою очередь исследователь Чернов А.А[[80]](#footnote-80) также отмечает, что важнейшую роль в становлении информационного общества играет правило и принцип ментальной идентичности. Иначе говоря, вход в новую для общества систему координат, вызвано это стремительным технологическим прогрессом, вынуждающим общество трансформироваться, или же другими условиями, которые не оставляют возможностей обществу для существования без
изменений, всегда подобный вход консолидирует общество, объединяет вокруг уже существующих морально-общественных устоев и идей.

Изучая описанный процесс перехода общества на примере Российской Федерации, автор данного исследования, отмечает, что для нашего государства переходные период формирует особую, отдельную систему социально=экономической направленности, направленную на длительную перспективу. Подобный вывод обосновывают обстоятельства, наличие которых присуще исключительно для России.

Во-первых, Российская Федерация – государство, образованное сравнительно недавно. При распаде государственного образования СССР в России сформировались уникальные национальные интересы, которые до сих пор многими партнерами по международному диалогу остаются не до конца понятыми. Многие государства мыслят ошибочными категориями, которые включают рассмотрение области геополитических и национальных интересов России либо как до сих пор не сформировавшимися, либо полностью наследуемыми от СССР. Исходя из этого, перед государственной информационной внешней политикой стоит задача по размеренному, всеобъемлющему, обоснованному, но устойчивому включению национальных интересов в систему международных, глобальных, региональных центров силы, соперничества и влияния.

Во-Вторых внутри государства, переход к новому политическому режиму, становление гражданского общества в процессе его трансформации, как в новое геополитическое образование, на новый социальный строй, во время включения страны в систему глобального информационного обмена формируется процесс смены устоявшихся принципов социальной ориентации, при чем по многим ключевым аспектам общественного мышления. Здесь и смена государственной идеологии для старших поколений, вступление в неизвестный информационный век, для нового поколения. Иными словами, перед рядовым гражданином Российской Федерации стоит задача по изменению своих принципов и процессов идентификации, как с внешним миром, так и с внутренним обществом, а так же сформировать отношения с политическим режимом и новыми формами общественных институтов. Подобные обстоятельства, в дополнении с традициями и устоями, сформировавшимися за время существования СССР, являются усложняющими обстоятельствами для перехода общества на «новые рельсы» информационного века. Осознание наличия подобных препятствий является ключевым фактором необходимым для понимания источникам принятия управленческих решений в области осуществления перехода общества.

Важный аспект информатизации общества на примере волеизъявления источника власти в стране: выборов в органы государственной власти и органы местного самоуправления рассмотрел в своей научной работе Е.В.Проценко[[81]](#footnote-81): «Выборы должны рассматриваться в качестве способа для комплектования органов государственной власти и органов местного самоуправления составом людей, которые по своим психологически-нравственным качествам являются пригодными для работы в подобных структурах», «В настоящий момент отсутствует структура обеспечивающая широкое общественное информирования не только по вопросам даты проведения выборов и списка кандидатов, но и обеспечивающая право участвовать компетентно, сознательно, для того, что бы выбраны были люди изначально готовые и пригодные
для подобной службы. Подытоживая освещение данного аспекта Е.В. Проценко отмечает,
что в настоящий момент существует необходимость влияния инициативой Президента
РФ и Государственной Думы для совершенствования нормативно-правовой базы выборов
и дополнения, которые будут направлены на устранение существующих перекосов
в избирательных компаний, которые мешают выборам выполнять своё прямое предназначение. Но процесс выборов является обоснованием обеспечения внутренней безопасности государства, говоря о внешней стороне вопроса, стоит отметить важность информационного взаимодействия с партнерами-государствами, подобные взаимодействия должны выстраиваться по принципу партнерских взаимоотношений. Таким образом, Российская Федерация интегрирует свои национальные интересы в систему глобальных взаимосвязей и взаимодействий. Политические руководства государств-партнеров, также как и политическое руководство нашей страны, обладают иерархией приоритетов выражающей их собственные политические интересы, отраженные в концепции национальной безопасности их государств. Приводя пример, можно вспомнить, как во времена развала СССР наличие общих приоритетов у США[[82]](#footnote-82) их партнеров по НАТО и Европейских государств, заставило их выделить определение «конфликтной политики»[[83]](#footnote-83), как отдельное направление внешнеполитического курса по отношению к Советскому Союзу. Проводя анализ материалов западной периодической, автор может констатировать что область исследования относительно экономических, социальных и общественных процессах, не чужда зарубежным исследователем, более того, во многих аспектах они демонстрируют высокую осведомленность, что позволяет сказать о широком «фронте» исследований, которому подвергаются практически все сферы жизнедеятельности нашего государства. Современные технологии дает возможность политологам и исследователям сформировать область знания, которая помогает прогнозировать развитие процессов внутри Российской Федерации. Понимание подобного рода, открывает возможность для управление данными процессами, возможность возникновения кризисов или конфликтов в различных сферах. Подобные механизмы информационного восприятия, обозначают, что специалисты, которые вовлечены в данный процесс, могут и передают своему руководству инструкции и механизмы, которые направлены на успешное и компетентное противостояние нашему государству в политическом, общественном и экономическом информационном противоборстве.

Именно высокий уровень информированности, подкрепленного материально-техническим обеспечением, позволяют противникам в информационной сфере ( США, НАТО и их союзникам), вносить коррективы в информационно-политическую стратегию, сперва в отношении Советского Союза, а после и России. Данная стратегия претерпела много изменений, в 50-х годах, использовалась определениями «массированного возмездия», что не удивительно, в те времена, основу стратегий национальной безопасности, во всех ведущих странах мира составляла доктрина термоядерного удара. Позднее стратегии претерпели изменения вплоть до «доктрины неоглобализма», а далее и вовсе НАТО озвучило стратегию развития, которая несет название «Партнерство во имя мира» и направлена на распространение Союзников на восток. Обоснование таких изменений является тем, что при распаде Советского Союза и формировании на его территории новых государственных образований и геополитических сил, в высших эшелонах власти США сформировалась концепция «контролирования конфликтов», а территория бывшего СССР[[84]](#footnote-84), была объявлена «зоной постоянных конфликтов». Не требуется глубокого анализа, что бы сформировать четкое понимание, что благополучие и устойчивое развитие нашего государства и стран СНГ не входит в планы и интересы наших заокеанских «партнеров». Свою силу и развитие они видят исключительно в разрушении социально-общественного строя, насильственной смене власти, дестабилизации обстановки и разрушение устойчивых горизонтальных политических связей на постсоветском пространстве, поскольку формирование сильной и экономически-развитой России – является прямой угрозой национальным интересам США. Исходя из вышесказанного, автор подчеркивает, что существует информационная угроза российскому государству, которая исходит от стран НАТО и приближенных к ним политических и неполитических акторов. Угроза заключается в формировании дестабилизирующих факторов, к которым стоит отнести:[[85]](#footnote-85)

- Предоставление актуальной и достоверной информации объектов безопасности, как внутренних, так и международных. Обладание неотъемлемым правом на получение информации о процессах и явлениях, которые интересуют данные объекты является обязательным процессом, который называется активная информированность, данный процесс обусловлен неотъемлемым правом обладать данной информации, в рамках законодательно-нормативных правовых актов, направленных на обеспечения секретности данных, попадающих под определение «секретности» или «тайны».

- Действия, которые направленны на формирование и поддержание правового вакуума в вопросах обеспечения, как информационной, так и других видов безопасности.

- Стимулирование предпосылок к политическим конфликтам, создание локальных и региональных кризисов, финансирование их, управление процессами, порождаемыми конфликтами, направление их, приведение к насильственной смене власти или режима как конечному результату.

- Формирование и создание положительных условий для отказов в области информационных систем, провоцирование отказов и сбоев в средствах технического обеспечения информационной безопасности.

- Действия и процессы, направленные на преднамеренное нарушение законодательства, нарушение общественного порядка в вопросах информационной безопасности.

В целях недопущения формирование подобных факторов, права и свободы граждан должны обеспечиваться законодательной базой, которая формируется и создается исходя из специфики условий современности, то есть учитывает особенность информационного воздействия и аспектов информационного противоборства. Существуют также права и свободы граждан в духовной сфере, которые выражены в неотъемлемой нужде индивидуумов в обогащении культурно-духовными ценностями. Права данной категории должны обеспечиваться законодательством, которое будет обеспечивать регулирование образования и функционирование организаций образовательного, религиозного и просветительного характера, а так же деятельность средств массовой информации, представленных, как в традиционном медиа-пространстве, так и в сети Интернет.

В формировании обеспечения информационной безопасности, главное сформировать единый принцип. В основе государственного формирования информационно защищенного общества лежит главный принцип: равной безопасности. Говоря об информационной сфере, можно констатировать трансформацию принципа равной безопасности в принцип адекватности информирования. Под адекватной информированностью, автор данного исследования понимает право всех государств на информационную безопасность и получение объективной информации, данный принцип учитывает интересы всех объектов информационной безопасности, гарантирует отсутствие дискриминации и исключает возможность получения односторонних преимуществ. Важное требование, которое формирует наличие верховенства права в информационной сфере, это требование к механизмам реализации верховенства права в информационной деятельности, а именно: каждый субъект информационного процесса для выполнения своих функций должен обладать сформированным правосознанием, являться законопослушным элементом и полностью представлять последствия своих действий, ровно как и ответственность, если данный субъект вступит в конфликт интересов или нарушит систему отношений внутри информационного взаимодействия, установленную правом на активное информирование.

Пути оптимизации обеспечения информационной безопасности, проистекают из определения исходящих угроз. Применение тех или иных способов обеспечения информационной безопасности, зависит от характера информационных угроз, а характеры делятся по вытекающему следствию действий субъектов информационных угроз, они могут быть неумышленные или умышленные. В первом случае, когда угроза вызвана неумышленными действиями субъектов информационного взаимодействия, обеспечение информационной безопасности осуществляется информационным патронатом и информационной кооперацией. Во втором случае, когда информационная безопасность государства ставится под угрозу из за умышленных действий субъектов, вовлеченных в информационный обмен, обеспечение равных ответов на угрозы осуществляется путем информационного противодействия со стороны государственной информационной политики.

Раскроем описанные определения более подробно. Информационный патронат подразумевает наличие у субъектов государственной информационной политики сведений о наличии дестабилизирующих факторах и угрозах. Причем механизм информационного патронат - подразумевает не только наличие и хранение информации, о наличии и классификации угроз, но и добывание подобных сведений, обмен ими между вовлеченными субъектами, то есть органами государственной власти и силовыми структурами. Информационная кооперация – процесс обеспечения информационной безопасности, который протекает в среде равных по своему значению, весу и структуре субъектов информационного процесса. Данный механизм включает в себя взаимосогласованные действия по обмену уже существующей у всех субъектов информации, относительно информационных угроз или же дополнение существующей у одних субъектов информации тем, у кого данная информация отсутствует. Информация может быть о дестабилизирующих факторах или же информационных угрозах, в редких случаях информация может содержать сведения о конкретных мероприятиях, которые направлены на дестабилизацию функционирование конкретного субъекта.

Положение Российской Федерации, в настоящее время – положение субъекта глобального информационного обмена, который только начал осуществление перехода к новым социально-экономическим отношениям. Подобное положение создает проблемы специфического характера. Сегодня для информационных служб, которые выполняют работу на иностранные правительства, приоритетной задачей является выявление и использование максимального возможного числа каналов информационного воздействия.

Подобный вывод, сформирован на основе анализа публикуемых исследований и документов, который показывает, что по сравнению с ранее публикуемыми документами, новые обладают детальным уровнем обобщения, а также присутствие довольно обширной базы фактологических данных. Именно эта особенность позволяет понять, что изучение социально-экономических процессов и политических аспектов нашей страны, все более базируется на анализе публикуемых работ наших соотечественников, то есть «внутренних» исследователей. Е.В. Проценко описывает это как: «осуществляется переход от самостоятельной аналитической обработки полученных первичных данных, к использованию аналитических материалов, которые представлены внутри информационной сферы государства, то есть происходит вовлечение альтернативных исследовательских структур».

 Особо стоит отметить вышеописанные факторы, учитывая условия отсутствия необходимого уровня материально-технического обеспечения на основе отечественных разработок, говоря другими словами: органы государственной власти вынуждены осуществлять закупки импортной техники и обеспечения механизмов привлечения иностранных фирм для осуществления материально технического обеспечения, в полной мере, которая необходима для нормального функционирования всех элементов информационного обмена.

Из-за использования технических средств и иностранных агентов при обслуживании повышается риск несанкционированного доступа внутрь системы информационного обмена, происходящего среди субъектов государственной информационной политики.

**3.2 Совершенствование системы обеспечения информационной безопасности**

Проведенный анализ основных направлений информационной безопасности Российской Федерации, позволяет сделать вывод, что наша страна находится на этапе создания и формирования стабильной защиты от информационных угроз. Процесс по созданию системы подобного рода долгосрочен и требует многих ресурсов. Учитывая происходящие в Российской Федерации социальные трансформации, необходимо уточнить, что под состоянием информационной безопасности страны понимается способность государства обеспечить достаточный уровень защищенности все слои гражданского общества от негативного информационного влияния и преступлений в информационной среде. Для Совершенствования системы обеспечения информационной безопасности необходимо всеобъемлюще и полно охарактеризовать опасность для Российской Федерации исходящую из информационной сферы. Современные технологии открывают широчайшие возможности для ведения информационного противоборства в социальной и политической сфере общества. Терроризм и действия противоправного характера сегодня возможны и в информационном поле, информационный терроризм, становится угрозой для государства, по опасности сравнимый с военными действиями или терактом на территории страны. Распространение нелегальных материалов, информации безнравственного характера, образование в сети Интернет объединений деструктивно влияющих на молодежь, повсеместная информационная экспансия, основанная на дезинформации и направленная на дискредитацию международного имиджа Российской Федерации, вот далеко не полный список угроз, с которыми столкнулось наше государство.

Имея полное и достоверное виденье угроз информационной безопасности Российской Федерации, можно выдвинуть ряд задач, основополагающих для совершенствования системы информационной безопасности нашей страны:

Необходимо разработать отдельные направления государственной политики в области обеспечения информационной безопасности. Считаю необходимым создать государственный орган по контролю за сетью Интернет, поскольку первым шагом к обеспечению достаточного уровня информационной безопасности страны, является предопределение информационных преступлений еще до того, как они могут быть совершены. Организованное ведомство предлагаю включить в введенье Министерства Обороны Российской Федерации, поскольку ФСБ, ФСО, Минкомсвязь и Роскомнадзор имеют слишком широкий спектр обязанностей и их деятельность связана не только с информационной сферой, что допускает возможность не достаточного уровня обеспечения информационной безопасности. Созданное подразделение Министерства Обороны Российской Федерации необходимо закрепить в нормативно-правовых документах, для создания правового основания для его функционирования. Направление деятельности ор**ганизо**ванного ведомства должно быть строго регламентировано и обращено на информационную сферу как внутреннюю, так и внешнюю. Подобному государственному органу можно поручить перечень задач по обеспечению информационной безопасности страны:

Обработка и анализ информационных потоков, имеющих широкую конечную аудиторию, на наличие информации разжигающей социальную или иную рознь, информации деструктивно влияющей на население и пресечение подобных источников информации.

Контроль и мониторинг деятельности иностранных информационных источников осуществляющих свою деятельность на территории Российской Федерации.

Обнаружение дезинформации или информации «сфабрикованного» характера и освещение подобных актов манипуляции в СМИ и сети Интернет[[86]](#footnote-86), с целью дискредитировать источники подобных «вбросов» перед широкой общественностью.

Отслеживание информационной сферы на предмет информации о возможных актах террора или других противоправных деяний и пресечение подобных действий[[87]](#footnote-87). Достоверное и полное освещение событий социальной, культурной и политической жизни Российской Федерации в сети Интернет на всех ключевых языках мира, с целью недопущения искажения фактов средствами массовой информации других стран.

Предоставление открытой и точной информации по острым социальным вопросам внутри страны с целью снижения градуса напряженности и увеличения доверия к государственным источникам информации со стороны населения. Организованную структуру необходимо наделить широкими полномочиями и организовать кооперацию с иными ведомствами и органами государственной власти для увеличения оперативности и продуктивности работы.

В целях совершенствования системы информационной безопасности перед ведомствами и структурами Российской Федерации, которые уже обеспечивают информационную безопасность страны, стоят следующие задачи: Обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям осуществляющим техническую разведку. Формирование и реализацию в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности.

Для совершенствования системы информационной безопасности Российской Федерации так же необходимо недопущение развития, следующих неблагоприятных факторов. Получение несанкционированного доступа иностранными государствами к информационной базе научно-технических исследований российских ученых.

Создание благоприятных условий на российском рынке для иностранной информационно-технической продукции, в условиях ограничения научно-технического потенциала, на рынке других государств. Постепенный вывод из сферы информационного влияния Российской Федерации стран ближнего зарубежья, расслоение единого информационного пространства государств-участников СНГ за счет переориентации на западные страны. Резкое снижение финансирование научных учреждений, разрабатывающих информационные технологии. Утечка за пределы Российской Федерации идеи, технологий и интеллектуального потенциала в данной области. Увеличение технологического разрыва между Россией и развитыми информационными странами. Первоочередной задачей в процессе совершенствования системы информационной безопасности является совершенствование законодательства Российской Федерации, регулирующего отношения в данной области и механизмов его реализации. Государству необходимо создать систему оценки возможного ущерба наиболее важным объектам обеспечения информационной безопасности страны.

Будущее системы обеспечения информационной безопасности Российской Федерации сталкивается с целым рядом проблем. К правовым проблемам в самом общем виде относится, нашедшее отражение во второй главе, данной исследовательской работы, несовершенство законодательной и нормативно-правовой базы, на основании, которой осуществляет свою деятельность система обеспечения информационной безопасности нашего государства. Существующие правовые нормы не позволяют перейти с бумажных на электронные носители во многих областях государственного управления, ввиду некой предубежденности, касающейся достоверности электронных документов, а следовательно, предъявлении особых требований к их защите. Отсюда следует, что одним из приоритетов развития является: совершенствование законодательной базы обеспечения информационной безопасности. При развитии данной отрасли права, следует обеспечить гласность и открытость разрабатываемых проектов в информационной сфере[[88]](#footnote-88). Создание надлежащих условий для использования электронных документов в государственном управлении. В процессе внедрения и развития информационно-коммуникационных технологий в системе публичного управления США столкнулись со следующими проблемами: стратегия информационно-коммуникационных технологий, принятая изначально, носила децентрализованный характер, отсутствовал контроль и координация проектов по использованию и развитию собственных начинаний и идей, что вылилось в отсутствие формальных институтов обеспечения деятельности всей информационно-коммуникационной сферы.

Особенностью Российской Федерации является не наличие собственных проблем, возникающих при становлении информационного общества и управления данным обществом в условиях глобализации, а масштабность решаемых задач по внедрению и необходимость мобилизации значительных ресурсов для их решения[[89]](#footnote-89). В условиях глобализации, построения с нуля рыночной экономики, необходимости повышения уровня жизни населения, выделить необходимое количество ресурсов на развитие информационно-коммуникационных технологий было крайне сложно.

Такое положение было актуально для первой половины становления государственности нового типа в Российской Федерации. В настоящее время, когда ситуация в стране стала более стабильной и имеется возможность выделения ресурсов на развитие и обслуживание столь сложной системы связи, как информационно-коммуникационная, именно в этом направлении необходимо мобилизовать государственные ресурсы.

Теоретически это позволит создать систему, не только обеспечивающую достаточный уровень информационной безопасности государства, но и информационную систему взаимодействия государства с обществом. А также между отдельными ведомствами, что позволит сэкономить на административных и транзакционных издержках, а также повысить эффективность деятельности органов государственной власти, а так же ведомств по обеспечению информационной безопасности. Даже те меры, которые были предприняты в рамках реализации концепции формирования электронного правительства в 2008-2010[[90]](#footnote-90)г, давшие возможность сформировать единое информационно-электронное пространство в Российской Федерации, по своему объему работ трудоемкие и сложные, не позволили нам получить лидирующие позиции в рейтинге готовности стран к «электронному правительству», где сейчас мы занимаем 27-е место (уточним, что Стратегией развития информационного общества в Российской Федерации была поставлена цель войти в топ-20 к 2020 году).

В рамках данной исследовательской работы, на основании проведенного анализа системы информационной безопасности Российской Федерации, можно сформулировать ряд рекомендаций, относящихся к приоритетам развития системы информационной безопасности:

**Рекомендация 1:** Совершенствование, дополнение и дальнейшая разработка нормативно-правовой базы государственной политики информатизации. Законодательство Российской Федерации в области государственной политики информатизации – разрозненный многоэлементный механизм, в котором существует ряд проблем. Предлагается внести изменения в действующее законодательство в части обеспечения информационной безопасности. Учреждение новых ведомств, чья деятельность будет направленна исключительно на обеспечение достаточного уровня информационной безопасности страны. Крайне необходимо закрепить, зарекомендовавший себя порядок государственно-частного партнерства в сфере информационно-коммуникационных технологий.

**Рекомендация 2**: Повышение уровня образования в области информационных технологий, расширение исследований в данной сфере на базе отечественных вузов и исследовательских центров. Увеличение государственного финансирования подобных инициатив. Стимулирование развития информационных технологий через государственно-частное партнерство и органы международной кооперации.

**Рекомендация 3**: Устранение технического дисбаланса в системе информационно-коммуникационных связей внутри государства, обеспечение сотрудничества между органами власти разного уровня. Обеспечение интеграции различных баз данных в единую точку доступа, информационный центр, в целях обеспечения межправительственного взаимодействия между субъектами и федеральным уровнем.

**Рекомендация 4:** Усиление уровня безопасности подобного информационного центра государственного взаимодействия, в целях недопущения вредоносного воздействия на него извне.

**3.3 Освещение новейших течений в области политической коммуникации и информационного взаимодействия.**

В заключительном параграфе данной исследовательской работы, автором освещаются новейшие течения, которые возникают или осуществляют свое развитие на данный момент. Подвергая данные процессы анализу, они будут раскрыты как понятия и описаны угрозы, возникающие в процессе из функционирования, в контексте данной магистерской диссертации.

Виртуальные частные сети (Virtual Private Network «VPN»). По своей сути виртуальные частные сети являются технологией для подключения конечного пользователя или пользователей к удаленной сети. Структура VPN включает как отдельные каналы информационного взаимодействия внутри глобальной сети, так защищенные протоколы взаимодействия и маршрутизаторы. Как работает данная система? Предположим у корпорации или компании существуют несколько локальных сетей одного уровня, для объединения их в единую виртуальную сеть используются отдельные каналы внутри глобальной сети. При реализации объединения используется механизм туннелирования. Инициатор объединения запускает пакеты локальной сети и пакеты немаршрутизируемых протоколов в вновь созданные IP-пакеты, в исходный код которых прописывается адрес инициатора и адрес получателя туннеля. При получении входящей информации туннельным способом, адресатом осуществляется процесс извлечения исходного пакета в обратной последовательности. Для обеспечения конфиденциальности передаваемой информации, также используются протоколы шифрования при передачи информации. Иначе говоря два носителя информации, к примеру персональных компьютера, находящиеся на большом расстоянии друг от друга организуют закрытый канал связи, через доступные общественные сети. Для чего применяется столь сложные технические наработки и какие угрозы это может создать для информационного взаимодействия?

Во-первых, подобные механизмы применяются для маркировки участников сетей и информации, что бы избежать смешивание информационных потоков и разделение их по принципу «свой-чужой».

Во-вторых, со времен первых способов передачи информации на расстояния, сразу с развитием средств по передаче информации, развивались и средства её шифрования, одним из которых и является VPN.

В-третьих в частных сетях, и сетях обменивающихся информацией содержащей в себе корпоративную, государственную или личную тайну, необходимо поддерживать целостность и замкнутость подобной сети, как от внешних проникновений в систему, так и от внутренних попыток информацию из этой системы вывести.

Но в российском обществе подобные механизмы информационного обмена нашли, особое применение[[91]](#footnote-91). Программное обеспечение, разработанное для смартфонов, функционирующих на операционных системах iOS и Android и предоставляющее технологию туннельного подключения к виртуальным частным сетям, позволяет обойти существующий фильтр информации. Что позволяет получить доступ к информационным материалам, экстремистского, террористического, сексуального, насильственного и других типов запрещенного на территории РФ содержания. Подобная технология, может позволить злоумышленникам обмениваться зашифрованной информацией. Организациям, в чьи цели входит подрыв нравственно-моральных устоев российского общества, получения возможности на транслирование информации через виртуальные частные сети, защищенные протоколами шифрования есть панацея от практически всех инструментов обеспечения информационной безопасности Российской Федерации. Раскрыв понятие еще пока нового для мировой общественности процесса, согласно отчету GlobalWebIndex в 2018 году для доступа к социальным сетям VPN использовали около 230 млн человек, автор обосновывает, что неподконтрольное осуществление технологического процесса VPN: является гипотетической угрозой информационной безопасности государства.

The Onion Router «TOR». – это приложение, фактически это браузер для взаимодействия с информационно-коммуникационной сетью интернет, структура, которого не позволяет отследить исходящий адрес подключения. Система использует сеть частных компьютеров, на которых она установлена, чаще их именуют узлами, которые в хаотичном и зашифрованном порядке пересылают и повторно шифруют исходящий трафик. Разработкой данной системы начали еще в 1990-х годах, те же исследователи, которые породили своим трудом всемирную глобальную информационную сеть Интернет: Американское федеральное Агентство DARPA. Запуск браузера TOR произошел в 2002 году, в отличии от всемирной паутины у браузера нет регулятора или управляющего, тысячи программистов по всему миру консолидируют свой труд что бы исключить возможные лазейки и уязвимости системы. Как работает данная система? При подключении к сети Интернет поток данных передается от источника подключения (вашего компьютера или смартфона) к сайту к которому вы обращаетесь. Происходит информационная связь. По своей структуре сеть Интернет является открытым и свободным пространством (в большинстве своём), позволяющее объемам данных свободно передвигаться от источника подключения к адресу его запроса и обратно. Именно свободность и открытость данной системы является уязвимостью через которую, исходящий или входящий трафик, можно перехватить, или даже перенаправить.

Браузер TOR с первого момента инициализации информационного запроса у источника подключения направляет трафик исключительно через свои внутренние узлы (компьютеры по всему миру на которых установлено данное программное обеспечение), каждый из которых обладает собственными кодами шифрования. Специфика подобного информационного исключает возможность раскрытия адреса исходящего запроса и конечного адреса запроса, поскольку внутренние узлы, которые обслуживают данный запрос не имеют данных об источнике запроса.

Для наглядного понимания специфики работы данной системы, автор приведет пример работы в данном браузере. Инициатор информационного обмена находится в г. Москва Россия, он обращается к данным расположенных на сайте www.example.com домен которого обслуживается серверами компании: «Hosting.Co» с фактическим расположением в Осло Норвегия. При использовании обычных интернет браузеров схема подключения выглядит следующим образом:

IP адрес 91.77.81.79 Россия, Москва, отправляет пакеты данных и получает ответ от IP адреса 193.90.12.86 Осло Норвегия. Прямой, прослеживаемый и открытый информационный обмен. Теперь же как это выглядит при использовании браузера TOR. Изначально информационное взаимодействие начинается с условного сайта, на январь 2019 года этим сайтом являлся https://search.disconnect.me – обращение к данному сайту выстраивает цепочку шифрования вашего запроса, а именно, на выходе «Hosting.Co» получает запрос, который прослеживается как

Бельгия 37.194.59.47 – Германия 213.61.66.117 – США 216.17.99.183, получается за вас ваш запрос выполняют другие участники браузера TOR, причем информационную составляющую они раскрыть не могут, они обладают только информацией о дальнейшем адресате, то есть адрес в Бельгии о направлении в Германии, а тот о адресе в США, который в свою очередь направляет запрос в Норвегию, не обладая информацией о том очередное ли это «перенаправление» или конечный адрес запроса откуда пойдет ответ. Пытаться отследить информационный трафик, транслируемый через браузер TOR бесполезно и невозможно. Да существует вероятность инфицирования конечного адресата вирусом или создание его полного двойника, то есть «фишинга», тогда мы получим в наше распоряжение содержание информационного запроса, но его адресат так и останется неизвестным. А при использовании TOR+VPN даже такая возможность исключается, поскольку финальная информационная сеть будет связана шифрованным «туннелем» и инициатором информационного обмена. Подобным образом формируется Анонимная передача данных, вокруг которой и на материально-технических ресурсах браузера TOR формируется «Даркнет». Теневая сторона Интернета, в который невозможно подключится или войти не используя протоколов шифрования браузера TOR иначе говоря, информационная площадка защищенная от возможных вмешательств, утечки информации или информационного вторжения, доступ к которой осуществляется монопольно через браузер TOR. В чем же угроза и опасность функционирования такой площадки. В условиях анонимности и невозможности отслеживания информационного трафика, на ресурсах Даркнета осуществляется продажа средств запрещенных к гражданскому обороту, среди которых наркотические, психотропные вещества, оружие, детская порнография, запрещенная литература, поддельные документы. Также возможно осуществление деятельности по торговле людьми, обмену криптовалют, обналичиванию средств, осуществлению заказных убийств. Это не цитата из научной фантастики. Это реальность сегодняшнего дня. Достаточно приобрести любой смартфон с выходом в интернет что бы получить доступ к торговой площадке, предоставляющей доступ к абсолютно всем запрещенным законодательством РФ видам услуг и товаров. Единственным ограничителем стоит то, что сеть беспроводного доступа к сети Интернет или чип сим-карты все еще можно дешифровать и взломать. Но и это последнее ограничение, вскоре будет снято. Тезисы и факты, которые были обоснованы, позволяют автору отнести функционирование системы TOR к реальным угрозам не только информационной, но и национальной безопасности.

Сеть околоземных спутников Starlink для обеспечение высокопроизводительного спутникового интернет-канала связи, покрывающего всю планету. Данная сеть, является разработкой компании SpaceX, а именно отделом по разработке и исследованию интернет-коммуникаций расположенном в США штат Вашингтон. Система спутниковой связи, была представлена в январе 2015 года. Оценочная пропускная способность, системы – 50% всего интернет трафика на планете. 22 февраля 2018 года, на орбиту было выведено два спутника Tintin-A и Tintin-B. 24 мая 2019 года на орбиту было выведено 60 спутников глобального интернета Starlink. Для обеспечения работоспособности системы необходимо наличие 12 000 спутников на околоземной орбите. Отношения международных субъектов в космосе регулируется Договором о космосе от 1967г. Данный документ регламентирует деятельность государств в космическом пространстве и указывает на невозможность ведения военных действий в космосе. На сегодняшний день на околоземной орбите находится порядка 5 тысяч искусственных спутников, в том числе уже завершивших свой срок службы. Каждая страна обладает собственным частотным диапазоном, на котором осуществляются работы систем связи и коммуникации. В России для военных и гражданских частот зарезервированы определенные частотные диапазоны, использование, которых регулируется военным ведомством страны. Даже вывод на коммерческий рынок связи формата 4G, долгое время согласовывался операторами именно с Минобороны России. Первая угроза, которую формирует проект Starlink – это угроза столкновения искусственных спутников на околоземной орбите. Поскольку Starlink – это не единственная компания, которая готовится к выводу своих спутников на околоземную орбиту, среди прочих6 Blue Origin, Samsung, Boeing. Суммарное количество спутников превысит 20 000 штук. Вторая угроза формируется из юрисдикции этих компаний ни одна из них не является государственной, а значит что кто первый зарезервирует для своей компании территорию ближайшего космоса – тот и станет вещать на большинстве доступных частотах, остальным придется либо перекупать частоты, либо искать другие варианты взаимодействия. Третья и являющейся основной угрозой исходит из цели программы: трансляции интернета на территории всей планеты, подобные механизмы, должны осуществляться исключительно при согласовании с правительствами всех стран и ООН.

**Заключение**

В данной исследовательской работе, был проведен анализ системы обеспечения информационной безопасности Российской Федерации, в условиях осуществления политической и других видов коммуникации во всемирной сети Интернет. На основе данного анализа, можно сделать вывод, что именно данное направление государственной, как внешней, так и внутренней политики Российской Федерации, является на сегодняшний день, одним из приоритетных. От реализации данного направления зависит в дальнейшем, и внутренние благополучия, и внешний престиж нашей страны. Эффективность обеспечения информационной безопасности в современном мире, предопределяет роль государства в мировой политике. С амбициями Российской Федерации на внешнеполитических фронтах реализации государственной политики, подобному вопросу опасно уделять недостаточно внимания. Реализация мер по усилению системы информационной безопасности в нашей стране началось с первой половины 2000-х годов, на тот период российская внешняя политика осуществила наиболее значимые изменения, причиной к которым, стало трансформация постсоветского пространства и нарастающее давление со стороны внешнеполитических соперников.

В этих условиях Российская Федерация начала реализовывать политическую стратегию по укреплению присутствия в мировом информационном пространстве. В данной работе был проведен анализ подобных действий, позволяющий сделать следующие выводы.

Во-первых, документальное закрепление государственной информационной политики Российской Федерации, на данный момент находится в не завершенном этапе. Впереди еще множество кардинальных реформ и преобразований. Необходимость совершенствования нормативно-правовой базы, озвучивалась неоднократно. Многие вопросы требуют закрепления в законодательном пространстве. Доктрина информационной безопасности Российской Федерации, стала основой для реализации задач и целей внешней политики России, связанных с защитой внутреннего информационного пространства нашей страны и распространением достоверной и открытой информации за пределами России

Данный документ не является всеобъемлющим, но развитие доктринальных оснований обеспечения информационной безопасности, несомненно происходит, это наглядно показывает различия между Доктриной информационной безопасности 2000 и 2016 года. Разработка подобных обширных и основополагающих нормативно-правовых актов, является признаком позитивного развития всей системы, обеспечения информационной безопасности Российской Федерации. Помимо вопросов, затрагивающих внутреннее информационное пространство страны, Доктрина информационной безопасности может обеспечить усиление формирование единого информационного пространства с союзными государствами. Указанная доктрина может быть использована в качестве примера и модели для формирование нормативно-правовой базы обеспечения информационной безопасности Республики Беларуси, Казахстана и Киргизии, учитывая немаловажное обстоятельство, что внешнеполитические стратегии наших стран имеют многие общие векторы развития.

Во-вторых, впервые за много лет, государственная политика обращает внимание на безопасность личности. Информационно-коммуникационные связи, не могут и не должны угрожать ценностям и правам закрепленным в Конституции Российской Федерации. А неприкосновенность личной информации и личной жизни, несомненно относится к таковым. До настоящего времени у нашего государства попросту не было необходимых технических и человеческих ресурсов для всеобъемлющего и полного обеспечения личностного уровня информационной безопасности. Полными потенциалами Россия не обладает и сейчас, но обращение к данной проблеме, поиск путей оптимизации и решения её, уже говорят о стабилизации ситуации в области защиты прав и свобод внутри нашего государства.

В-третьих, угрозы и опасности в области обеспечения информационной безопасности страны, ставят задачи перед научно-техническим и военно-промышленным комплексом страны. Отставание в информационно-техническом обеспечении Российской Федерации, мобилизует все мощности для наращивания производства средств информационно-коммуникационной связи, обмена и перехвата.

В-четвертых, информационная политика Российской Федерации в настоящее время нацелена на формирование благоприятного имиджа нашего государства за рубежом. Для этого используется структуры внешнеполитического и внешнеэкономического государственного аппарата. Подобная деятельность связана с обескураживающим уровнем анти-российской пропаганды и дезинформации как в Средствах массового информирования, так и в информационно-коммуникационной сети Интернет. К сожалению, на данный момент
анти-российские настроения, с подачи США, звучат все чаще и громче. Особой задачей при противостоянии подобной информационной экспансии, стоит недопущение искажения исторического наследия нашей страны. Уже сейчас во многих европейских учебных заведениях формируется заведомо ложная историческая действительность, молодежь не знает кто одержал победу в Великой Отечественной Войне и какой ценой. Роли Союзников преувеличиваются, а Советского Союза преуменьшается. Подобная динамика при бездействии со стороны Российской Федерации, может привести к исчезновению упоминаний о героическом прошлом нашей страны со страниц учебников, что будет еще одной информационной победой Соединенных Штатов Америки. Решение подобных проблем является задачей для современной российской дипломатии. Необходимость поддержки использовании русского языка в странах ближнего и дальнего зарубежья, а также изучении российской истории в различных государствах. Осуществление подобных задач наталкивается на проблемы связанные с недостатком финансирования за рубежом.

В-пятых, необходимость формирования конкурентоспособной информационно-технической базы в Российской Федерации, озвучено еще в первой Доктрине информационной безопасности, а вопросам необходимости формирования профессионального кадрового состава в сфере обеспечения информационной безопасности государства, уделяется крайне мало внимания. Между тем именно человеческий ресурс предопределяет успех прогнозирования и раскрытия информационных опасностей на раннем этапе. Вопросу подготовки и квалификации кадров информационной безопасности необходимо уделить как можно больше внимания, поскольку формирование производств информационно-технических средств и подготовка специалистов, в той же области неразрывно связаны.

На основе сформированных выводов, можно выделить основные направления, требующие особого внимания в системе обеспечения информационной безопасности:

* Использование всех ведомств и структур государственного аппарата в пропаганде российского образа жизни, достоверном и открытом освещении традиций, истории и культуры Российской Федерации за пределами нашего государства.
* Использование новых информационных технологий с целью воздействия на общественное мнение, как в целях внутренней, так и внешней государственной политики Российской Федерации.
* Формирование новых и реорганизация старых производственных мощностей, с целью сокращения разрыва в техническом оснащении нашей страны.
* Использование новых информационных технологий для недопущения несанкционированного доступа и проникновения в информационное пространство Российской Федерации.

Анализируя вышеизложенное, можно сформировать заключение.

С появлением новых информационных технологий, вызвавших усложнение информационного обмена между людьми, внедрение информационных технологий во все сферы жизнедеятельности современного общества, повсеместное использование средств информационно-технического обмена и сетей информационно-коммуникационного направления, ставит нас перед фактом, что обеспечение информационной безопасности если не сегодня, то в ближайшем будущем станет первостепенным вопросом системы безопасности любого государства. Количество информационных потоков растет, а качество падает. Присутствие источников и потребителей информации с каждым днем увеличивается, что увеличивает угрозу информационного терроризма в разы. Один квалифицированный хакер способен нанести ущерб, сопоставимый с боевой операцией, реализуемой целым военным ведомством отдельной страны. При это препятствие для подобной операции, которым в прошлом являлось территориальное расположение государств, больше не имеет значения. Для производства информационного оружия не требуется государственного финансирования, построения заводов и военно-промышленной поддержки. Производство информационного оружия, даже совместными усилиями всех государств невозможно поставить под контроль.

Следовательно, перед Российской Федерацией стоит задача сформировать организационно-правовую систему, способную по своей технической и материально-ресурсной составляющей, координировать развитие информационно-коммуникационной инфраструктуры внутри нашей страны, подробный анализ и разработку направлений отражения угроз и опасностей информационной безопасности страны

**Список использованных источников и литературы**

**Источники:**

Концепция национальной безопасности России, утвержденную Указом Президента РФ от 17.12.97 № 1300

Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

Указ Президента Российской Федерации № 260 от 22 мая 2015 года «О некоторых вопросах информационной безопасности Российской Федерации».

Приказ Россвязькомнадзора № 996 от 05 сентября 2013 г. «Об утверждении требований и методов по обезличиванию персональных данных»; Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи».

Указ Президента Российской Федерации № 170 от 20 января 1994 года «Об основах государственной политики в сфере информатизации» (в ред. Указов Президента РФ от 26.07.95 № 764, от 17.01.97 № 13, от 09.07.97 № 710).

ФСБ России. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ РФ 21 февраля 2008 г. №149/6/6-622).

1. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями от 27 июля 2010 г.) // Собрание законодательства Российской Федерации. 2006. №31 (часть I). Ст. 3448.
2. Концепция государственной информационной политики Российской Федерации.

Концепция формирования информационного общества в Российской Федерации.

Доктрина информационной безопасности Российской Федерации.

1. The Global Enabling Trade Report 2008. World Economic Forum, Geneva, Switzerland 2008

The Research and Discussion on Effectiveness Evaluation of Software Protection // 12th International Conference on Computational Intelligence and Security (CIS). 2016

**Литература**

1. Шампань, П. Делать мнение. Новая политическая игра Текст. / П. Шампань. М., 1997. - 335с
2. Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. 2014.
3. Цыгичко В. Н., Смолян Г. Л., Черешкин Д. С. Информационное оружие как геополитический фактор и инструмент силовой политики. М.: ИСА РАН, 1997.
4. Хачатуров К. А. Обеспечение внешнеполитических позиций России в свете Доктрины информационной безопасности Российской Федерации. В сб.: Внешнеполитическая информация и современная дипломатия. Дипломатическая академия МИД России. 2010.
5. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями от 27 июля 2010 г.) // Собрание законодательства Российской Федерации. 2006. №31 (часть I). Ст. 3448
6. Указ Президента РФ от 31.12.2015 №683 «О Стратегии национальной безопасности Российской Федерации».
7. Указ Президента РФ от 16.08.2004 №1082 «Вопросы Министерства обороны Российской Федерации

Указ Президента РФ от 11.08.2003 №950 «Вопросы Федеральной службы безопасности РФ»

1. Указ Президента РФ от 07.08.2004 №1013 «Вопросы Федеральной службы охраны Российской Федерации»
2. Спивак, Д. JL Измененные состояния массового сознания Текст. / Д. Л. Спивак. Спб., 1996
3. Сельченок, К. В. Контроль сознания и методы подавления личности.
4. Расторгуев С.П. Философия информационной войны. 2010

Путин. В.В. Быть сильными: гарантии национальной безопасности для России.

1. Проценко, Е.В. Информационная безопасность политической коммуникации в современной России.: дис. канд. полит. наук. 2011
2. Почепцов, Г. Г. Коммуникативные технологии двадцатого века Текст. / Г. Г. Почепцов. М.: Рефл-бук, 2009
3. Постановление Правительства Российской Федерации от 02.06.2008 №418 «О Министерстве связи и массовых коммуникаций Российской Федерации»
4. Послание Федеральному Собранию Российской Федерации Президента России Владимира Путина Текст. //Российская газета, 2007, 27 апреля
5. Обращение Дмитрия Медведева к участникам «РИФ+КИБ 2012»
6. Концепция национальной безопасности Российской Федерации Текст. // Независимое военное обозрение. 2000. № 1.
7. Кокошин А. А., О стратегическом планировании в политике. М.: КомКнига, 2007 г
8. Классификация угроз несанкционированного доступа к «охраняемому информационному ресурсу» в автоматизированных информационных системах органов внутренних дел / А. Д. Попов [и др.] // Моделирование систем и процессов. -2017. - Т. 9. - № 4. - C. 55-58.
9. Кикоть-Глухоедова Т.В. Анализ понятий «система национальной безопасности» и «система обеспечения национальной безопасности». 2015
10. Калиткин Н. Н. Численные методы / Н. Н. Калиткин. - Москва : Наука, 1978. - 512 с.
11. Информационные вызовы национальной и международной безопасности. Под общей ред. А.В.Фёдорова и В.Н.Цыгичко. Библиотека ПИР-Центра 2001.
12. Информационное оружие - новое средство обеспечения национальных интересов. Тамбов: МИНЦ, 2001,- С.5-8
13. Илюшкин С.Ю. Некоторые аспекты понятий «информационное обеспечение» и «Информационное обслуживание» 2010
14. Зиновьев П. В. Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса при её проектировании в системах электронного документооборота : монография / П. В. Зиновьев, И. И. Застрожнов, Е. А. Рогозин. - Воронеж : Воронеж. гос. техн. ун-т, 2015. -106 с.
15. Заславская Т.И. О социальном механизме посткоммунистических преобразований в России // Социол. исслед. 2002. № 8. С. 3-16.

Закон Российской Федерации «О безопасности», 5 марта 1992 г. ст. 13

1. Жужлов А.А. Гражданское общество современной России в условиях медиатизации политики: дис. канд. пол. наук. Саратов, 2013

Еремичев Ф.С. Некоторые вопросы стратегии национальной безопасности как правовой основы обеспечения национальной безопасности России. 2016

1. Дубровин А. С. Общенаучные итоги создания эталонной модели защищенной автоматизированной системы / А. С. Дубровин // Фундаментальные исследования. - 2015. - № 2-15. - С. 3247-3251.
2. Дубровин А. С. Методы и средства автоматизированного управления подсистемой контроля целостности в системах защиты информации : монография / А. С. Дубровин [и др.] - Воронеж : Воронеж. гос. техн. ун-т, 2003. - 165 с.
3. Дровникова И.Г. Численные методы расчёта показателя эффективности вспомогательной подсистемы в системе электронного документооборота / Дровникова И.Г., Зиновьев П.В., Рогозин Е. А. // Вестник Воронежского института МВД России. - 2016. - № 4. - С. 114-121.
4. Дробин В. У. Надежность и эффективность в технике Т. 3: Эффективность технических систем / В. У. Дробин ; под общ. ред. В. Ф. Уткина, Ю. В. Крючкова. - Москва : Машиностроение, 1988. - 328 с.
5. Доктрина информационной безопасности Российской Федерации
6. Данные Исследовательского агентства Alexa Internet.// URL: http://www.alexa.com/
7. Григорьев В. А. Имитационная модель системы защиты информации / В. А. Григорьев, А. В. Карпов // Программные продукты и системы : международный журнал - Тверь : МНИИПУ и НИИ «Центрпрограммсистем», 2005. - № 2. - С. 26-30.
8. Грачев Г., Мельник И. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. М.: Институт философии РАН, 1999.
9. ГОСТР ИСО/МЭК 15408-2-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные компоненты безопасности.
10. ГОСТ РВ 15.307-2002. Военная техника. Испытания и приемка технических изделий. Основные положения [Электронный ресурс]. - URL: http//askbooks.ru/file/3880/download (дата обращения: 27.02.2018).
11. ГОСТ Р 51583-2014. Порядок создания автоматизированных систем в защищенном исполнении [Электронный ресурс]. - URL: http://docs.cntd.ru/document/1200108858 (дата обращения: 30.01.2018).
12. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения // СПС «КонсультантПлюс».
13. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения // СПС «КонсультантПлюс».
14. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования [Электронный ресурс]. - URL: http://www.internet-law.ru/gosts/gost/3436 (дата обращения: 31.01.2018).
15. ГОСТ 23773-88. Машины вычислительные, электронные, цифровые, общего назначения [Электронный ресурс]. - URL: http://docs.cntd.ru/document/1200016759 (дата обращения: 01.04.2018).
16. Горный Е. Летопись русского Интернета: 1990-1999.
17. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. - Москва : МИФИ, 1997. - 537 с.
18. Востоков Н. Квантовая криптография / Н. Востоков, С.Н. Борисова // Успехи современного естествознания. - 2012. - № 6. - С. 88-90.
19. Внешнеполитическая информация и современная дипломатия. Отв. редактор Ю. Б. Кашлев. Редактор Г. Н. Вачнадзе. М.: Дипломатическая академия МИД России, 2001.
20. Винокуров. И.Д. «Совершенствование национальной безопасности». ВКР РАНХиГС, СЗИУ 2016г.
21. Венцель Е. С. Теория вероятностей / Е. С. Венцель - Москва : Наука, 1969. -576 с.
22. Василенко Л.А. Информатизация системы государственной службы. Социологические аспекты.- М., 2002

Буравлев А.И. Сколько стоит национальная безопасность: к вопросу о расходах на обеспечения безопасности личности и государства. Вооружение и экономика. 2015.

1. Боэм Б. Характеристики качества программного обеспечения / Б. Боэм [и др.] ; пер. с англ. Е. К. Масловского. - Москва : Мир, 1981. - 208 с.
2. Бородакий Ю. В. Проблемы и перспективы создания автоматизированных систем в защищенном исполнении / Ю. В. Бородакий, А. Ю. Добродеев // Известия ЮФУ. Технические науки. - 2007. - № 4. - С. 3-6.
3. Боридьков И. С. Политика безопасности в субъектно-объектной модели безопасности информации в автоматизированных системах / И. С. Боридьков, Д. В. Смирнов // Известия института инженерной физики. - 2013. - Т.1. - № 27. –
4. Беляева О. В. Имитационное моделирование систем защиты информации / О. В. Беляева, В. А. Грицык // Международный журнал экспериментального образования. - Пенза : Академия Естествознания, 2010. -№ 5.- С. 67.
5. Безопасность как критерий информационного выбора России вXXI веке. Право и информатизация общества 2012

Баньков А.С. Информационное обеспечение национальных интересов Беларуси и России // Современные коммуникационные технологии в государственной информационной политике. Доклады и выступления на научно-практической конференции. 2013

1. Амосов А. А. Вычислительные методы для инженеров / А. А. Амосов, Ю. А. Дубинский, Н. В. Копченова. - Москва : Высшая школа, 1994. - 544 с.

Аминов И.Р, Сулейманов А.Р. Институционализация национальной безопасности в истории России: внешние и внутренние угрозы. Правовое государство: Теория и практика. 2014.

Средства массовой информации постсоветской России: Учебное пособие / Я. Н. Засурский, Е. JI. Вартанова, И. И. Засурский и др.; под ред. Я.Н. Засурского. - М.: Аспект Пресс, 2002.

Статья Стрельцова, А. А. Содержание понятия «Обеспечение информационной безопасности» / Информационное общество, 2001, вып. №4, с. 10-16.

Судоргин, О. А. Императивы и приоритеты политики обеспечения информационной безопасности России. Автореф. дис. ... канд. полит, наук. - М.: МГОУ, 2005

Тагарев, Т. Т. Томас о ключевых элементах русского подхода к информационной войне // Информация и безопасность. - София, 1998. - № 2. - С.75-92

Ткач, И. А. Разработка концепции информационной войны в интересах национальной безопасности // Информационная безопасность регионов России: Тр. конф. СПб., 2000.

Уэбстер, Ф. Теории информационного общества. - М.: Аспект Пресс, 2004. - 400 с.

Фатьянов, А. А. Правовое обеспечение безопасности информации в Российской Федерации: Учебное пособие. М.: Издательская группа «Юрист», 2001.-С.42

Федотова, JI. Н. Социология массовой коммуникации. — СПб.: Питер, 2003.-400 с.

1. Zaitsev D.A. Simulating Telecommunication Systems with CPN Tools: Students' book / D.A. Zaitsev, T.R. Shmeleva. - Odessa : ONAT, 2006. - 60 p.
2. Yan H. Power information systems security: modeling and quantitative evaluation / H. Yan, X. Xiaorong, X. Yaozhong // IEEE Power Engineering Society General Meeting. - 2004.
3. Xin Z. Research on effectiveness evaluation of the mission-critical system / Z. Xin, M. Shaojie, Z. Fang // Proceedings of 2013 2nd International Conference on Measurement, Information and Control. - 2013. - P. 869-873.
4. U.S. National Space Policy. White House. Washington DC. August 3
5. The Research and Discussion on Effectiveness Evaluation of Software Protection / H. Wang [et ol.] // 12th International Conference on Computational Intelligence and Security (CIS). - 2016. - P. 628-632.
6. The Global Enabling Trade Report 2008. World Economic Forum, Geneva, Switzerland 2008
7. Rogers. E. Communication technology: The new media in society. -New York, 1986
8. Richard Szafranski, A Theory of Information Warfare: Preparing for 2020 // Airpower Journal, Spring 1995, p. 25-35
9. Ptitsyn P. S. Designing architecture of software framework for building security infrastructure of global distributed computing systems / P. S. Ptitsyn, D. V. Radko, O. V. Lankin // ARPN Journal of Engineering and Applied Sciences. -2016. - Т. 11. - № 19. - P. 11599-11610.
10. Nikishin K. Implementation of time-triggered ethernet using colored Petri NET / K. Nikishin, N. Konnov, D. Pashchenko // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2017. - P. 1-5.
11. National Strategy to Secure Cyberspace. White House, Washington DC. September 2018
12. National Strategy for Homeland Security. Washington DC, White House, 2003
13. National Security Strategy of the United States 2002, White House Washington DC. 2002
14. My El Hassan Charaf. A colored Petri-net model for control execution of distributed systems / My El Hassan Charaf, Salma Azzouzi // 4th International
15. Method to Evaluate Software Protection Based on Attack Modeling / H. Wang [et ol.] // 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing Year. -2013. - P. 837-844.
16. McCall J. A. Factors in Software Quality: Metric Data Collection and Validation. Final Technical Report. Vol. 2 / J. A. McCall, P. K. Richards, G. F. Walters. - Springfield : National Technical Information Service, 1977.
17. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O. Hrvoje, G. Marin // Computers & Security. - 2015. - P. 100 -112.
18. Katrin Voltmer Mass media and political communication in new democracies. — London, 2006
19. Jensen K. Coloured Petri Nets. Modeling and Validation of Concurrent Systems. / K. Jensen, L. M. Kristensen. - Berlin : Springer-Verlag, 2009.
20. Critical Foundations Thinking Differently. Washington DC, White House, Office of the Press Secretary. October 22, 1997\
1. Соловьев, А. И. Политическая коммуникация: к проблеме теоретической идентификации. // Полис. - 2002. - № 3. - С. 5-18. [↑](#footnote-ref-1)
2. Пугачев, В. П. Средства массовой информации в современном политическом процессе // Вестник Московского университета. Сер. 12. Политические науки. - 1995. - №5. [↑](#footnote-ref-2)
3. Прокофьев, В. Ф. Тайное оружие информационной войны. М.: СИНТЕГ, 1999 (Серия «Информатизация России на пороге XXI века»). - С.34 [↑](#footnote-ref-3)
4. Расторгуев, С. П. Философия информационной войны. - М.: Вуз. кн., 2001.-468 [↑](#footnote-ref-4)
5. Попов, Г. Н. Переход России к информационному обществу. - СПб.: ООО ИПК БИОНТ, 2003. - 122 с. [↑](#footnote-ref-5)
6. Xin Z. Research on effectiveness evaluation of the mission-critical system / Z. Xin, M. Shaojie, Z. Fang // Proceedings of 2013 2nd International Conference on Measurement, Information and Control. - 2013. - P. 869-873 [↑](#footnote-ref-6)
7. O. V. Lankin // ARPN Journal of Engineering and Applied Sciences. -2016. - Т. 11. - № 19. - P. 11599-11610. [↑](#footnote-ref-7)
8. Nikishin K. Implementation of time-triggered ethernet using colored Petri NET / K. Nikishin, N. Konnov, D. Pashchenko // International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM). 2017. - P. 1-5 [↑](#footnote-ref-8)
9. Jensen K. Coloured Petri Nets. Modeling and Validation of Concurrent Systems. / K. Jensen, L. M. Kristensen. - Berlin : Springer-Verlag, 2009 [↑](#footnote-ref-9)
10. Серебрянников, В. В. Войны России. - М, 1998. - С.212-217; Дзлиев М. И., Урсул, А. Д. Основы обеспечения безопасности России. - М.: Экономика, 2003. - С. 309-356. [↑](#footnote-ref-10)
11. Зиновьев П. В. Методы и средства оценки эффективности подсистемы защиты конфиденциального информационного ресурса [↑](#footnote-ref-11)
12. Почепцов, Г. Г. Коммуникативные технологии двадцатого века. М.: Рефл- бук, К.: Ваклер, 2000. - С.55-84 [↑](#footnote-ref-12)
13. Проценко, Е.В. Информационная безопасность политической коммуникации в современной России.: дис. канд. полит. наук. 2011 [↑](#footnote-ref-13)
14. Василенко Л.А. Информатизация системы государственной службы. Социологические аспекты.- М., 2002 [↑](#footnote-ref-14)
15. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 // СПС «КонсультантПлюс» (дата обращения: 07.03.2019). [↑](#footnote-ref-15)
16. . Об утверждении Концепции обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года : приказ МВД России от 14.03.2012 №169 [↑](#footnote-ref-16)
17. Государственная программа «Информационное общество (2011–2020 годы)»

Утверждена постановлением Правительства от 15 апреля 2014 года №313. Действующая редакция госпрограммы «Информационное общество (2011–2020 годы)». [↑](#footnote-ref-17)
18. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. - Москва : МИФИ, 1997. - 537 с. [↑](#footnote-ref-18)
19. Л.Д. Рейман доклад на семинаре «Глобализация информационного пространства вызовы и новые возможности для России» [↑](#footnote-ref-19)
20. Прайс, М. Телевидение, телекоммуникации и переходный период: право, общество и национальная идентичность. - М.: Изд-во Моск. ун-та, 2000.-336 с [↑](#footnote-ref-20)
21. Попов, Г. Н. Переход России к информационному обществу. - СПб.: ООО ИПК БИОНТ, 2003. - 122 с. [↑](#footnote-ref-21)
22. Kresimir S. The information systems' security level assessment model based on an ontology and evidential reasoning approach / S. Kresimir, O. Hrvoje, G. Marin // Computers & Security. - 2015. - P. 100 -112 [↑](#footnote-ref-22)
23. Лопатин В.Н. «Информационная безопасность России: Человек. Общество. Государство. / Санкт-Петербургский университет МВД России. СПб.: Фонд «Университет», 2000 - 428 с. [↑](#footnote-ref-23)
24. Richard Szafranski, A Theory of Information Warfare: Preparing for 2020 // Airpower Journal, Spring 1995, p. 25-35 [↑](#footnote-ref-24)
25. Заславская Т.И. О социальном механизме посткоммунистических преобразований в России // Социол. исслед. 2002. № 8. С. 3-16. [↑](#footnote-ref-25)
26. Василенко Л.А. Информатизация системы государственной службы. Социологические аспекты.- М., 2012 [↑](#footnote-ref-26)
27. Доктрина информационной безопасности Российской Федерации. М.: Междунар. изд-во «Информациология» [↑](#footnote-ref-27)
28. Об основах государственной политики в сфере информатизации: Указ Президента РФ №170 от 20 января 1994 г. // Рос.газета. 1994. - 29 янв [↑](#footnote-ref-28)
29. Послание Федеральному Собранию Российской Федерации Президента России Владимира Путина Текст. //Российская газета, 2007, 27 апреля. [↑](#footnote-ref-29)
30. Концепция внешней политики Российской Федерации (подписана президентом РФ 12.07.2008 г.) Текст. / Российская газета, 2008, 26 мая [↑](#footnote-ref-30)
31. Концепция национальной безопасности Российской Федерации Текст. // Независимое военное обозрение. 2000. [↑](#footnote-ref-31)
32. Конституция Российской Федерации Текст.- офиц. текст. М.: Маркетинг, 200 [↑](#footnote-ref-32)
33. Аминов И.Р, Сулейманов А.Р. Институционализация национальной безопасности в истории России: внешние и внутренние угрозы. Правовое государство: Теория и практика. 2014 [↑](#footnote-ref-33)
34. Проект Конвенции об обеспечении информационной безопасности [↑](#footnote-ref-34)
35. Critical Foundations Thinking Differently. Washington DC, White House, Office of the Press Secretary. October 22, 1997 [↑](#footnote-ref-35)
36. National Strategy for Homeland Security. Washington DC, White House, 2003 [↑](#footnote-ref-36)
37. National Security Strategy of the United States 2002, White House Washington DC. 2002 [↑](#footnote-ref-37)
38. Пугачев, В. П. Средства массовой информации в современном политическом процессе // Вестник Московского университета. Сер. 12. Политические науки. - 1995. - №5 [↑](#footnote-ref-38)
39. Расторгуев, С. П. Философия информационной войны. - М.: Вуз. кн., 2001.-468 с. [↑](#footnote-ref-39)
40. National Strategy to Secure Cyberspace. White House, Washington DC. September 2018. [↑](#footnote-ref-40)
41. U.S. National Space Policy. White House. Washington DC [↑](#footnote-ref-41)
42. Rogers. E. Communication technology: The new media in society. -New York, 1986 [↑](#footnote-ref-42)
43. Данные Исследовательского агентства Alexa Internet.// URL: http://www.alexa.com/ [↑](#footnote-ref-43)
44. Горный Е. Летопись русского Интернета: 1990-1999. // URL: http:// www.zhurnal.ru/staff/gorny/ texts /ru\_let> [↑](#footnote-ref-44)
45. Информационные вызовы национальной и международной безопасности. Под общей ред. А.В.Фёдорова и В.Н.Цыгичко. Библиотека ПИР-Центра 2001. [↑](#footnote-ref-45)
46. Результаты исследования «W3Techs» 2017 [↑](#footnote-ref-46)
47. Прохожев, А. А. Методологические основы решения проблем внутренней безопасности России. Материалы науч. конф. "Проблемы внутренней безопасности России в 21 веке. -М.: ЗАО ЭДАС ПАК, 2001. - С.52 [↑](#footnote-ref-47)
48. Katrin Voltmer Mass media and political communication in new democracies. — London, 2006 [↑](#footnote-ref-48)
49. The Global Enabling Trade Report 2008. World Economic Forum, Geneva, Switzerland 2008 [↑](#footnote-ref-49)
50. Пугачев, В. П. Средства массовой информации в современном политическом процессе // Вестник Московского университета. Сер. 12. Политические науки. - 1995. - №5. [↑](#footnote-ref-50)
51. Ptitsyn P. S. Designing architecture of software framework for building security infrastructure of global distributed computing systems / P. S. Ptitsyn, D. V. Radko, O. V. Lankin // ARPN Journal of Engineering and Applied Sciences. -2016. - Т. 11. - № 19. - P. 11599-11610. [↑](#footnote-ref-51)
52. Безопасность как критерий информационного выбора России вXXI веке. Право и информатизация общества 2012 [↑](#footnote-ref-52)
53. Илюшкин С.Ю. Некоторые аспекты понятий «информационное обеспечение» и «Информационное обслуживание» 2010 [↑](#footnote-ref-53)
54. Информационные вызовы национальной и международной безопасности. Под общей ред. А.В.Фёдорова и В.Н.Цыгичко. Библиотека ПИР-Центра 2001 [↑](#footnote-ref-54)
55. Сельченок, К. В. Контроль сознания и методы подавления личности Текст. / К. В. Сельченок. -М., 2001. [↑](#footnote-ref-55)
56. Спивак, Д. JL Измененные состояния массового сознания Текст. / Д. Л. Спивак. Спб., 1996 [↑](#footnote-ref-56)
57. Шампань, П. Делать мнение. Новая политическая игра Текст. / П. Шампань. М., 1997. - 335с [↑](#footnote-ref-57)
58. Method to Evaluate Software Protection Based on Attack Modeling / H. Wang [et ol.] // 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing Year. -2013. - P. 837-844. [↑](#footnote-ref-58)
59. .Указ Президента РФ от 11.08.2003 №950 «Вопросы Федеральной службы безопасности РФ»

Указ Президента РФ от 07.08.2004 №1013 «Вопросы Федеральной службы охраны Российской Федерации» [↑](#footnote-ref-59)
60. .Указ Президента РФ от 16.08.2004 №1082 «Вопросы Министерства обороны Российской Федерации [↑](#footnote-ref-60)
61. Постановление Правительства Российской Федерации от 02.06.2008 №418 «О Министерстве связи и массовых коммуникаций Российской Федерации [↑](#footnote-ref-61)
62. Указ Президента РФ от 07.08.2004 №1013 «Вопросы Федеральной службы охраны Российской Федерации». [↑](#footnote-ref-62)
63. Концепция государственной информационной политики Российской Федерации [↑](#footnote-ref-63)
64. «Концепция государственной информационной политики Российской Федерации.» [↑](#footnote-ref-64)
65. Буравлев А.И. Сколько стоит национальная безопасность: к вопросу о расходах на обеспечения безопасности личности и государства. Вооружение и экономика. 2015. [↑](#footnote-ref-65)
66. Об информации, информационных технологиях и о защите информации : федеральный закон от 27.07.2006 № 149-ФЗ (в ред. от 19.12.2016) // СПС «КонсультантПлюс» (дата обращения: 23.12.2017). [↑](#footnote-ref-66)
67. Илюшкин С.Ю. Некоторые аспекты понятий «информационное обеспечение» и «Информационное обслуживание» 2010 [↑](#footnote-ref-67)
68. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента РФ от 05.12.2016 № 646 // СПС «КонсультантПлюс» (дата обращения: 07.03.2019 [↑](#footnote-ref-68)
69. Смирнов, А. И. Проблемы международной информационной безопасности и внешняя политика России. "Информационная безопасность и внешняя политика России в 21 веке". [↑](#footnote-ref-69)
70. Росошанский, А. В. Система информационной безопасности СМИ в со временной России [↑](#footnote-ref-70)
71. Володенков С.В. «Особенности интернета как современного пространства для политических коммуникаций» 2014 [↑](#footnote-ref-71)
72. Кокошин А. А., О стратегическом планировании в политике. М.: КомКнига, 2007 г. [↑](#footnote-ref-72)
73. Проблемы преодоления «цифрового неравенства» в России и странах СНГ. Материалы международного семинара. М.: Дом Правительства РФ, 28 ноября 2000 г.-С.47 [↑](#footnote-ref-73)
74. Принципы, касающиеся международной информационной безопасности. Проект. Материалы МИД РФ, 2000 [↑](#footnote-ref-74)
75. Почепцов, Г. Г. Коммуникативные технологии двадцатого века Текст. / Г. Г. Почепцов. М.: Рефл-бук, 2002 [↑](#footnote-ref-75)
76. Eriksson, J. International Relations and Security in the Digital Age (Routledge Advances in International Relations and Global Politic). New York.: Routledge. 2007 [↑](#footnote-ref-76)
77. Egan, Mark, Mather, Tim. The Executive Guide to Information Security: Threats, Challenges, and Solutions. New-York. Addison-Wesley Professional. 2004. [↑](#footnote-ref-77)
78. Davis, Richard. The Web of Politics: The Internet's Impact on the American Political System New York: Oxford University Press, USA. 1999 [↑](#footnote-ref-78)
79. Боридьков И. С. Политика безопасности в субъектно-объектной модели безопасности информации в автоматизированных системах / И. С. Боридьков, Д. В. Смирнов // Известия института инженерной физики. - 2013. [↑](#footnote-ref-79)
80. Чернов А.А. Становление глобального информационного общества: проблемы и перспективы. 2014. [↑](#footnote-ref-80)
81. Проценко, Е.В. Информационная безопасность политической коммуникации в современной России.: дис. канд. полит. наук. 2011 [↑](#footnote-ref-81)
82. Federal Information Security Act of 2002 P.L. 107-347 [↑](#footnote-ref-82)
83. A Summary Guide: Public Law, Executive Orders, And Policy Documents. Department of the Treasury Deputy Assistant Secretary (Information Systems). CIO Office of Security. November 13, 2001 [↑](#footnote-ref-83)
84. Средства массовой информации постсоветской России: Учебное пособие / Я. Н. Засурский, Е. JI. Вартанова, И. И. Засурский и др.; под ред. Я.Н. Засурского. - М.: Аспект Пресс, 2002. - 303 с. [↑](#footnote-ref-84)
85. Critical Foundations Thinking Differently. Washington DC, White House, Office of the Press Secretary. October 22, 1997 [↑](#footnote-ref-85)
86. Дубровин А. С. Общенаучные итоги создания эталонной модели защищенной автоматизированной системы / А. С. Дубровин // Фундаментальные исследования. - 2015 [↑](#footnote-ref-86)
87. 46. Классификация угроз несанкционированного доступа к «охраняемому информационному ресурсу» в автоматизированных информационных системах органов внутренних дел / А. Д. Попов [↑](#footnote-ref-87)
88. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения // СПС «КонсультантПлюс». [↑](#footnote-ref-88)
89. Беляева О. В. Имитационное моделирование систем защиты информации / О. В. Беляева, В. А. Грицык // Международный журнал экспериментального образования. - Пенза : Академия Естествознания, 2010 [↑](#footnote-ref-89)
90. Проблемы преодоления «цифрового неравенства» в России и странах СНГ. Материалы международного семинара. М.: Дом Правительства РФ, 28 ноября 2000 г.-С.47 [↑](#footnote-ref-90)
91. Жужлов А.А. Гражданское общество современной России в условиях медиатизации политики: дис. канд. пол. наук. Саратов, 2013 [↑](#footnote-ref-91)