САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ШЕВЕЛЕВ Артём Андреевич

**ПРАВОВЫЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ КАК НОВЫЙ ПРИОРИТЕТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**THE POLICY OF LAW IN CYBER SECURITY AS A NEW PRIORITY IN NATIONAL SECURITY OF RUSSIAN FEDERATION**

Выпускная бакалаврская квалификационная работа

по направлению 031900 - Международные отношения

Научный руководитель -

кандидат политических наук,

старший преподаватель И.Е. Нестерова

Студент:

Научный руководитель:

Работа представлена на кафедру

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017 г.

Заведующий кафедрой:

Санкт-Петербург

2017

**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ…………………………………….…….…………………………….…………3

ГЛАВА I. СОВРЕМЕННОЕ СОСТОЯНИЕ КИБЕРБЕЗОПАСНОСТИ

* Сущность термина «кибербезопасность»…….…………………………………………15
* Основные угрозы информации и информационной инфраструктуре…………………22
* Правовые аспекты вопроса………………….……………….……..…………………….29

ГЛАВА II. МЕТОДОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ КИБЕРБЕЗОПАСНОСТИ

* Современные механизмы противодействия угрозам кибербезопасности…….….……41
* Будущее кибербезопасности в правовом поле…….…….…….……….…….…….……50

ГЛАВА III. КИБЕРБЕЗОПАСНОСТЬ КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

* Состояние и уровень информационной защищённости Российской Федерации……..56
* Отечественное законодательство во взаимодействии с международным правом…….62

ЗАКЛЮЧЕНИЕ……………………………………………………………………………….73

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ……………………79

**ВВЕДЕНИЕ**

«Кибербезопасность - это совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями»[[1]](#footnote-2). Данная формулировка вместе с Концепцией стратегии кибербезопасности Российской Федерации, впервые озвученные в ноябре 2013 года на заседании Совета Федерации, являются первым весомым результатом заложенной военно-политическим руководством страны ещё в далёком 2012 году политики, ключевым приоритетом которой выступило формирование прогрессивной нормативно-правовой базы в области регулирования киберпространства[[2]](#footnote-3). Рассмотрение исторической основы и перспектив развития обозначенной политики стало фундаментом исследования в области правовых аспектов обеспечения кибербезопасности.

Современные мир всё более утопает в технологиях. Привычные вещи перестают иметь свой первозданный вид. Многое перемещается в столь таинственное для большей части населения планеты электронное пространство, невидимое глазу и неосязаемое, но столь значимое для всего общества.

Его значимость берёт свои истоки от зарождения феномена интернета, который приобрёл известный нам облик лишь в середине 1990-х годов[[3]](#footnote-4), приведя к колоссальному сдвигу не только в области распространения и хранения информации, но и в сфере функционирования, как частных, так и государственных институтов. Интернет, как общедоступная платформа, стал первым шагом на пути в век информационных технологий. Всё большее число компаний и государственных органов стало переходить на электронный документооборот, с каждым днём увеличивая интеграцию технологий в повседневную рутину. Вскоре документооборот перестал быть единственной задачей электронного пространства, и на первый план вышел термин информация в его наиболее широком смысле, включающем в себя всё великое разнообразие материальных и нематериальных человеческих благ, перемещающихся или находящихся в электронном пространстве. Всё: от простого стационарного компьютера до масштабной информационной инфраструктуры международной компании, от загруженной в социальную сеть фотографии до базы данных федеральной службы безопасности - всё это примкнуло к понятию информации, выведя его на совершенно иной уровень, создав принципиально новую сферу для человеческой деятельности и коммуникации.

Теперь информация стала наиболее очевидным механизмом функционирования и двигателем эволюции общественных институтов. Однако, с повышением уровня интеграции у человечества появилась не только возможность ускорить темпы собственного развития, но и возникли новые слабые места: возникла новая сфера, безопасность которой, ввиду столь глубокой интеграции в человеческую и общественную жизнь, вышла на первый план для всего поколения. Угрозы безопасности информации и информационным ресурсам перешли в раздел определяющих безопасность и свободу человека: поддержание конституционных прав на свободу и неприкосновенность, на защиту достоинства личности и многие другие стало напрямую зависеть от сохранения порядка в информационной среде[[4]](#footnote-5). Впрочем, вышеупомянутый высокий уровень человеческой интеграции в эту самую среду требовал более чёткого уяснения области для взаимодействия, по этой причине был введён термин киберпространство, выступающий совокупностью не только технологических ресурсов информационной среды, но и учитывающий прямое воздействие человека на электронное пространство[[5]](#footnote-6).

Концентрируя вокруг себя великое множество объектов и сетей телекоммуникаций, киберпространство стало полноценным плацдармом для ведения борьбы, обладая всеми свойственными для того чертами: наличие заинтересованных в достижении личных целей акторов, механизмов для реализации данных целей и, что наиболее важно, наличие материальных благ, борьба за которые зачастую способна привести к большей выгоде, нежели непосредственные боевые действия. Учитывая подобное свойство киберпространства, становилась очевидной необходимость защиты информационной среды. Первое упоминание на международном уровне о подобной необходимости датируется ещё 1999 годом, когда на ежегодной конференции учёных в сицилийском городе Эриче были озвучены перспективы развития человечества в предстоящем XXI веке, среди которых были отмечены и наиболее значимые угрозы. Акцент производился на информационном, кибернетическом характере надвигающегося столетия, в котором первостепенная опасность исходила именно от киберпространства[[6]](#footnote-7).

Выраженные на конференции 1999 года опасения относительно угроз принципиально нового характера подтвердились уже в 2000 году, когда в сети появился нашумевший вирус «I love you», нанёсший пользователям суммарный ущерб более чем на 10 млрд долларов[[7]](#footnote-8). Тогда правительства всего мира начали выработку прогрессивных механизмов противодействия угрозам киберпространства, среди которых помимо привычных технических средств особое значение имело правовое регулирование сферы. В конечном счёте, зародившийся в середине 90-х годов прошлого столетия феномен на современном этапе качественно преобразовался: киберпространство встало в один ряд с такими областями ведения боевых действий как наземные, воздушные, морские[[8]](#footnote-9), чему напрямую способствовал технических прогресс человечества: с появление новых технологий возникают и новые средства воздействия на кибернетическую среду, а значит возникает и новая угроза информационной и кибербезопасности.

Прогресс остановить невозможно, а потому технологическое противоборство в киберпространстве также не имеет конца: на каждое действие, под которым в данном случае понимается создание безопасных сетей, баз данных, многоуровневых слоёв защиты, будет находиться своё противодействие в виде изобретения новых средств внедрения, поглощения или же уничтожения информации, а также средств непосредственного воздействия на её носитель. Тогда, получается, что «безопасность в сети» - это утопия? Отнюдь, не всё столь безнадёжно, как это может выглядеть со стороны: основной задачей всех технических средств, задействованных в киберпространстве, является реакция на возникающую угрозу, которая может быть выражена либо в виде оборонительных, либо в виде атакующих, превентивных, действий. В то время как основная задача по поддержанию кибербезопасности ложится на правовую сферу, которая призвана препятствовать зарождению угрозы, а не реагировать на конкретные последствия её проявления.

Таким образом, в сравнении с весьма непростой технологической базой, обеспечивающей безопасность киберпространства, правовое поле должно носить ещё более сложный и витиеватый характер, ввиду более комплексной задачи, стоящей перед данным рубежом обороны. На современном этапе национальными правительствами и такими международными организациями как ООН предпринят ряд правовых мер, среди которых особо выделяется принятие следующих документов: Стратегия действий в киберпространстве министерства обороны Соединённых Штатов, Конвенция ООН об обеспечении международной информационной безопасности, Доктрина информационной безопасности Российской Федерации, Резолюция Генеральной Ассамблеи ООН о Создании глобальной культуры кибербезопасности, Резолюции Генеральной Ассамблеи ООН о создании правовой основы для борьбы с преступным использованием информационных технологий и многие другие. Все они несомненно образуют массивный плацдарм для реализации проектов в области киберпространства, однако правовая база всё ещё испытывает нехватку прогрессивных мер, ограничивающих возможность вредоносных субъектов воздействовать на среду извне.

Подобный недостаток отчасти может быть обусловлен узконаправленностью принимаемых актов, прежде всего выраженной в области распространения принимаемых мер: основная работа ведётся с целью обеспечения национальной безопасности, а потому редко учитывает возможность международного сотрудничества и выдвижения комплексных международных мер по противодействию угрозам, что, учитывая неоднородность явления, в некотором смысле схожую с терроризмом[[9]](#footnote-10), исключительно создаёт ряд барьеров на пути вредоносных субъектов в киберпространстве, однако вовсе не препятствует их развитию. Даже при доскональном рассмотрении принимаемых Организацией Объединённых Наций нормативных документов видно, что большая часть из них носит некий рекомендательный для национальных правительств характер, выступая виде наставления по организации собственных действий в киберпространстве и не учитывая возможных последствий за его нарушение.

Рассмотренная свыше краткая ретроспектива развития киберпространства и его восприятия мировым сообществом говорит о необходимости выработки принципиально новых методов поддержания кибербезопасности, одним из которых могло бы служить создание обособленного международного органа, носящего не только рекомендательных характер, но и обладающего правом выдвижения определённых санкций в отношении государств, нарушающих принятые международные принципы во области поддержания мировой безопасности.

Таким образом, *актуальность* рассмотрения, анализа и выдвижения вероятных сценариев прогрессивного развития законодательной базы в области регулирования киберпространства не только на национальном уровне, но и на международном, не может быть поставлена под сомнение. Особенно принимая во внимание технический прогресс, в некоторых областях «переросший» существующую нормативно-правовую базу[[10]](#footnote-11), а также нарастание напряжённости в отношениях между государствами, напрямую связанных с киберпространством, о чём свидетельствует череда международных скандалов вокруг взлома электронной почты высокопоставленных политических деятелей, вскрытия конфиденциальной базы данных политических и общественных организаций[[11]](#footnote-12). Наиболее свежим и актуальным примером подобного воздействия на киберинфраструктуру, приведшего к обострению мировой обстановки, могут послужить события президентской гонки в США и во Франции, где основной ущерб был нанесён штабу Хиллари Клинтон[[12]](#footnote-13) и Эмануэля Макрона[[13]](#footnote-14), соответственно. Сообщается, что в обоих инцидентах прослеживается «Российский след», однако убедительных доказательств тому не приводится, что создаёт дополнительные дискуссии не только в вопросе причастности тех или иных стран к отмеченными инцидентам, но и в целом о возможности оказания решающего влияния на внутригосударственные процессы через киберпространство, а также о необходимости пресечения подобного воздействия.

Перечисленные свыше события и особенности явления кибернетического пространства позволили сформулировать основную *цель* исследования, которая заключается в рассмотрении феномена кибербезопасности прежде всего со стороны его нормативно-правового регулирования и в выделении вероятных сценариев эволюции области права, отвечающей за киберпространство. Особое внимание было уделено Российской Федерации и национальному законодательству государства, как одной из мировых стран, инфраструктура которой наиболее подвержена угрозам киберсреды[[14]](#footnote-15). При этом к *объектам* исследования, помимо упомянутой свыше нормативной базы, были также отнесены государственные и международные институты, причастные к её выработке и исполнению принятых правовых актов.

На пути реализации поставленной цели был выдвинут ряд первостепенных *задач*, выполнение которых позволило в полной мере раскрыть проблематику кибербезопасности и окружающей данный феномен правовой среды. К наиболее значимым из низ относятся:

1) Дать подробную характеристику феномена кибербезопасности с выделением основных угроз киберпространства

2) Сопоставить понятия кибербезопасности и национальной безопасности, а также выявить степень взаимозависимости явлений

3) Определить основные методы воздействия на киберпространство, производя акцент на правовое поле, однако учитывая технологический прогресс

4) Выработать чёткую картину восприятия кибербезопасности и киберпространства как такового в российском обществе, среди высшего военно-политического руководства и экспертного сообщества страны

5) Спрогнозировать вероятный путь эволюции механизмов регулирования киберсреды, а также смоделировать ряд прогрессивных мер, способных положительно повлиять как на национальный уровень кибербезопасности в Российской Федерации, так и снизить количество угроз общемировой киберсреде.

Помимо того входе изучения и анализа феномена кибербезопасности были рассмотрены существующие технические средства, системы, обеспечивающие необходимый уровень защищённости индивида, общества, государственных институтов и международных формирований от посягательств со стороны вредоносных субъектов киберпространства. Подобная оценка была произведена с целью наглядной демонстрации превосходящего значения нормативно-правовой области над существующими техническими средствами, задействованными национальными службами безопасности.

Среди промежуточных задач также особую роль сыграл вопрос о необходимости взаимодействия национального законодательства и национальных институтов с их зарубежными аналогами, а также на международном уровне. Отдельное внимание было уделено международному сотрудничеству государств в области формирования наднационального института регулирования международной правовой системы в области обеспечения мировой кибербезопасности, а также вероятной роли Российской Федерации в подобного рода межгосударственном формировании.

*Методологическую основу* исследования в большей степени составили теоретические методы изучения. Данный факт обуславливается первостепенной значимостью рассмотрения документальных источников и формирования определённой гипотезы на основании совокупности полученных сведений. По этой причине особо востребованными оказались методы изучения и обобщения, а также анализа и синтеза, которые позволили сделать несколько значимых выводов в области существующей нормативно-правовой системы, регулирующей киберпространство. Также немалую пользу оказали такие методы, как идеализация и абстрагирование, которые вкупе с методом экспериментально-теоретического уровня, моделированием, предоставили возможность решить одну из основных задач исследования, а именно: спрогнозировать вероятный путь эволюции механизмов регулирования киберсреды, а также смоделировать ряд прогрессивных мер, способных положительно повлиять как на национальный уровень кибербезопасности в Российской Федерации, так и снизить количество угроз общемировой киберсреде. Помимо упомянутых свыше методов, дополнительный вес вынесенным в ходе написания исследовательской работы заключениям предал метод сравнения, позволивший на практическом примере убедиться в их достоверности и в достоверности проведённой аналитической работы, а также, что наиболее важно, позволивший сопоставить уровень эффективности действующей в том или ином государстве технической базы по противодействию вероятным угрозам киберсреды с существующей в рассматриваемом регионе законодательной базой, выделив как положительные, так и отрицательные стороны оказываемого на кибербезопасность влияния от основополагающих факторов её формирования.

Как уже было отмечено свыше, формирование привычной нам сети «интернет» берёт своё начало в середине 90-х годов XX столетия[[15]](#footnote-16), по этой причине анализ киберпространства и его роли в национальной безопасности основывается на той документально-правовой и событийной базе, которые сформировались в большей степени уже непосредственно в XXI веке. Данный факт, с одной стороны, свидетельствует о том, что появляется возможность получить более точные и свежие сведения из области кибербезопасности, однако, с другой стороны, ограничивает и усложняет процесс сбора информации ввиду существования малого количества фундаментальных исследований в проблематике. Что, впрочем, в очередной раз подтверждает необходимость подробного рассмотрения сферы кибербезопасности с позиции формирования действенной нормативно-правовой системы, а также указывает на актуальность исследования.

Тем ни менее, не взирая на нехватку фундаментальных трудов российских и зарубежных специалистов в области безопасности по проблематике киберпространства и его регулирования, на современном этапе сформировалась уже достаточно широкая *источниковая база*, основу которой составляют международные и национальные нормативно-правовые акты, а также труды российских и зарубежных исследователей, отражающие отличные друг от друга взгляды на современное состояние и перспективы развития кибербезопасности.

В основу данной исследовательской работы вошли как нарративные, так и документальные источники. Каждая из перечисленных групп оказала особое влияние на реализацию изначально поставленной цели: сформулированные в ходе её анализа задачи требовали привлечения как фактологического материала, так и оценочного, дабы более полно и точно отразить действительную картину состояния кибербезопасности на международном и национальном уровнях. Так, к примеру, анализ Резолюций Генеральной Ассамблеи Организации Объединённых Наций по «Борьбе с преступным использованием информационных технологий» за номером 55/63 и 56/121 от 2001 и 2002 года соответственно, а также по «Созданию глобальной культуры кибербезопасности» за номером 57/239 от 2003 года позволил выявить основные мотивы и задачи, которыми руководствовалась Организация, выступая первостепенным институтом контроля и влияния на киберпространство в международной среде. Это также позволило, как отмечалось свыше, установить характер принимаемых в ООН и её специализированных подразделениях документов, которые в по большей части носят исключительно наставительный характер, демонстрируя государствам определённые меры, следуя и принимая которые планируется поддерживать дееспособность и безопасность мировых сетей. В тоже время нормативно-правовые и внутренние документы Организации Североатлантического договора, такие как Стратегическая концепция по обороне и безопасности членов Североатлантического договора, а также документы Объединённого центра передовых технологий киберобороны НАТО, свидетельствуют о стремлении организации любыми мерами гарантировать безопасность собственных членов, что многие специалисты характеризуют как действие политики «Hard Security» проводимой организацией и характеризующейся возможностью применения силы при необходимости[[16]](#footnote-17). Таким образом организация, с целью защиты собственных интересов, а также собственной инфраструктуры стран, исходя из собственной нормативно-правовой базы вправе воздействовать на информационную инфраструктуру противника. Соотношение понятий «hard power» и «soft power» будет подробно рассмотрено в одной из глав основной части исследовательской работы.

Продолжая тематику рассмотрения источниковой базы проведённого исследования нельзя не отметить влияние нарративных источников. Безусловно, как отмечалось ранее, на современном этапе проблематика кибербезопасности не изобилует фундаментальными исследованиями, впрочем это не означает, что их нет совсем. Превосходным примером подобной работы может послужить творение профессора Дипломатической академии МИД России М.Б. Касеновой[[17]](#footnote-18), в 2013 году опубликовавшей исследование получившее название «Кибербезопасность и управление интернетом». Данное издание в некотором смысле носит показательный для российских государственных органов характер, демонстрируя прогрессивные шаги применяемые за рубежом и подчёркивая грамотные нововведения, встречающиеся в отечественных институтах, связанных с обеспечением безопасности киберпространства. Помимо фундаментальных исследований, также немалую роль в формировании принципиально важных заключений сыграли публикуемые в научных и научно-популярных журналах, а также в интернет пространстве статьи. Рассмотрение источников подобного рода позволило проследить эволюцию технологической и законодательной базы как в Российской Федерации, так и в её зарубежных аналогах киберинфраструктуры. Среди данной группы источников особый вес имеют работы Ю.В. Бородакия[[18]](#footnote-19), А.Ю. Добродеева[[19]](#footnote-20), М.М. Безкоровайного[[20]](#footnote-21), А.В. Казаковцева[[21]](#footnote-22) и некоторых других специалистов в области безопасности и киберпространства. Так, к примеру, рассмотрение современных методов противодействия угрозам кибербезопасности в первую очередь основывалось на их характеристике со стороны вышеупомянутых специалистов, ввиду наличия в их трудах компетентной оценки рассматриваемого феномена.

В дополнение к вышесказанному следует отметить, что комплексный анализ источниковой базы указал на существование определённой исторической связи между инцидентами в киберпространстве, затрагивающими информационную инфраструктуру определённых государств или даже регионов, с повышением интереса академических кругов к проблематике, что на практике выражает в виде повышения количества публикаций научно-исследовательских работ в рассматриваемой области. Данный факт позволил выделить несколько этапов, ознаменовавших эволюцию общественной мысли в отношении феномена кибербезопасности, которые в дальнейшем будут более подробно разобраны с учётом технического прогресса и эволюции правовой базы:

- Май 2000 года. Выявление вируса «I love you». Данный инцидент привёл к активизации деятельности правительств в области кибербезопасности. Зарождение феномена.

- Апрель 2007 года. Кибератаки на информационную инфраструктуру правительства Эстонии. Выделение особой роли человеческого фактора в функционировании киберсреды. Внедрение механизмов политической борьбы в киберпространство.

- 2009 - 2010 года. Публикация миллионов документов на сайте международной некоммерческой организации WikiLeaks. Международный бум общественного сознания. Принятие рядом правительств принципиально новых стратегий информационной безопасности.

- Конец 2016 года. Публикация личных данных кандидата в президенты Соединённых Штатов Америки Хиллари Клинтон, а также взлом конфиденциальных ресурсов Демократической партии США и последовавшие за этим обвинения в адрес русских хакеров, предположительно работавших по заказу правительства страны. Возрождение активной дискуссии по проблематике безопасности киберпространства в общественных и правительственных кругах разных стран.

Безусловно, выше были перечислены далеко не все события киберпространства, имевшие колоссальный резонанс в обществе. Впрочем, даже упомянутых инцидентов должно быть достаточно для демонстрации факта углубления понятия кибербезопасности наравне с эволюцией феномена и изменением характера киберугроз, возникающих на определённых исторических этапах.

*Новизна* затрагиваемой тематики прежде всего исходит от характера технического и человеческого прогресса: сегодня - это уже не то, что было вчера, сегодня техническая и правовая база обеспечения кибербезопасности уже не та, которой она была пару дней назад. Изменение и выработка новых методов хищения, искажения и уничтожения информации и информационных ресурсов задействованных в киберпространстве требуют принятия принципиально новых контрмер. С изменением среды происходит и изменение характера киберпространства, а потому большинство исследований опубликованных в последнее десятилетие теряют свою актуальность, оставаясь весомыми лишь в качестве анализа исторической ретроспективы, а предложенные в них модели прогрессивного развития феномена становятся неприменимыми. Помимо того, исследования прошлых лет уделяли колоссально малое внимание рассмотрению моделей международного контроля киберпространства, а именно созданию обособленного наднационального органа по поддержанию безопасного состояния среды. При этом, существующие международные институты НАТО, занимающиеся кибербезопасностью или же киберобороной, как гласит название подразделения, впервые будут рассмотрены не в качестве объединяющего международного актора, гарантирующего безопасность мировой инфраструктуры, а скорее в качестве обособленного субъекта, также как и человек, способного пагубно воздействовать на киберсреду, а потому данное формирование не будет учитываться при построении вероятной модели международного контроля киберпространства, поскольку потребует от членов Североатлантического договора примкнуть к данной системе самостоятельно. Более того, в данной работе будет осуществлена попытка сформулировать необходимые к принятию на национальном и международном уровнях принципиально новые правовые нормы, способные благоприятно отразиться на общем состоянии и развитии мировой системы кибербезопасности, которая на современном этапе выступает совокупностью национальных систем кибербезопасности.

В случае успешной реализации поставленной цели и сформулированных задач, а также при формировании целостной модели, учитывающей обозначение необходимых мер, от принятия которых будет зависеть характер развития феномена киберпространства, теоретическая значимость работы может быть выражена в использовании академическим сообществом фундаментальных суждений, выработанных в ходе исследования с целью дальнейшей работы в области рассматриваемой проблематики. Также определённую практическую ценность будет представлять ни раз упомянутая модель прогрессивного развития правовой базы, которая должна стать финальным аккордом всего исследования и послужить примером для российских и зарубежных институтов, задействованных в выработке и реализации нормативно-правового фундамента кибербезопасности.

**ГЛАВА I. СОВРЕМЕННОЕ СОСТОЯНИЕ КИБЕРБЕЗОПАСНОСТИ**

**Сущность термина «кибербезопасность»**

Зарождение интернета на ровне с появлением аналогичных революционных технологий, вроде колеса, велосипеда, самолёта, радио-связи и многих других вещей, привело к качественному переосмыслению человеческих возможностей по индивидуальному и общественному развитию. Вместе с приходом новых возможностей, как уже отмечалось, появлялись и новые вызовы безопасности человека. По этой причине, зарождение киберпространства вместе с появлением интернета логичным образом вызвало формирование феномена кибербезопасности, в качестве ответной реакции на возникновение угроз совершенно иного характера[[22]](#footnote-23). Следовательно, для того, чтобы выявить действительную сущность термина «кибербезопасность» требуется провести доскональный анализ, как явления киберпространства, так и близких к нему понятий: информационной безопасности, информационного пространства, кибератаки, киберпреступности, кибертерроризма и некоторых других явлений.

Безусловно, формирование подобного рода сети, интернета, произошло гораздо раньше чем в 90-е годы, однако, прежде данная технология воспринималась как нечто недоступное, поскольку проект по формированию единой системы моментальной передачи данных, получивший грандиозную поддержку правительства Соединённых Штатов в 60-е годы XX века, в период наиболее обострённого положения на мировой арене, предназначался исключительно для военного пользования[[23]](#footnote-24). Особую роль в переходе военного ресурса в ранг общедоступного механизма сыграла передача технологий распространения информации в руки научного сообщества европейской части планеты. Данное событие произошло как раз на стыке веков и кардинальным образом изменило представление человечества о новоявленной сети передачи данных, количество пользователей которой кратно возросло всего за несколько лет: в начале 90-х годов XX века было зарегистрировано всего порядка 20 тысяч пользователей сети, в то время как на момент начала нового столетия, в 2000 году данное число возросло до 1 миллиарда человек[[24]](#footnote-25).

Информационная структура нового поколения не только набирала популярность среди общественности, но и день ото дня расширялась, принимая на себя новые функции, вышедшие за рамки передачи информации: хранение, редактирование, а также многие другие функции стали доступны пользователям в онлайн-режиме в ходе развития киберпространства, однако каждую из них в конечном счёте можно использовать не только на благо. Благодаря глубокой интеграции политических, социально-общественных, бизнес структур в электронное пространство, вредоносное воздействие на их дееспособность стало одной из основных угроз, исходящих от инфраструктуры киберсреды. Тогда экспертным сообществом всего мира началась выработка общей школы трактования угроз и действий по их упреждению в киберпространстве, с целью разработки более эффективных механизмов по противодействию вредоносным субъектам среды.

Однако, уже на данном этапе эксперты в области информационных технологий столкнулись с некоторыми трудностями: по мере развития киберпространства, среда принимала всё более неоднородный характер. В отличие от информационного пространства, выступающего совокупностью информационных ресурсов, влияющих на них операций по формированию, изменению и распространению массивов данных, а также учитывающее области возможного применения конечного продукта[[25]](#footnote-26), понятие киберпространства требовало учёта несколько дополнительных и при этом непостоянных субъектов, способных воздействовать на данный информационный фон: человека и технику[[26]](#footnote-27). Подобные субъекты, отличительной чертой которых выступает непостоянство воздействия на среду, наряду с высокой степенью влияния, в конечном счёте привели к схожей с определением понятия терроризма проблематике, когда основной объект изучения не перманентен и неоднороден, а потому не поддаётся точному трактованию и заключению в определённые нормативно-правовые и научно-детерминиционные рамки.

Вероятно, сравнение феномена кибербезопасности с феноменом терроризма будет ещё ни раз встречаться в ходе прочтения данной исследовательской работы. Впрочем, возвращаясь рассмотрению сущности понятия «кибербезопасность», как уже было отмечено свыше, международному сообществу не удалось прийти к согласию в вопросе общего восприятия феномена. Тем ни менее экспертные круги отдельных стран всё же достигли некоторых успехов в данном направлении, что несомненно благоприятно отразилось на методике построения национальной безопасности с учётом новых вызовов и угроз. К примеру, в американских академических кругах понятие кибербезопасности принято связывать с совокупностью принимаемых мер, проводимых мероприятий, а также действующих в киберпространстве институтов, главной целью которых является защита национальных информационных сетей, национальных систем, поддерживающих функционирование инфраструктуры, и самой информации от кибератак и возможных угроз киберсреды[[27]](#footnote-28). Подобный подход обоснован стремлением к поддержанию национальной обороноспособности страны и нашёл отражение в принимаемых высшим военно-политическим руководством государства нормативно-правовых актах. К примеру, предельно схожее трактование феномена кибербезопасности можно найти в принятой в апреле 2015 года Министерством Обороны Соединённых Штатов Стратегии кибербезопасности, в которой также делается акцент на защите информационной инфраструктуры Министерства Обороны и необходимости гарантии безопасности мирному населению страны[[28]](#footnote-29).

Переходя к рассмотрению позиций европейского экспертного сообщества, стоит отметить взгляд турецкого специалиста в области безопасности М. Карамана на феномен кибербезопасности, представленный в научно-популярной статье под названием «Institutional Cybersecurity from Military Perspective» или «Перспективы институционального развития кибербезопасности для военных ведомств». В своей работе, автор подчёркивает значимость создания не только технических средств защиты киберсреды, но и необходимость построения многоуровневой системы национальных институтов, обеспечивающих дееспособность киберинфраструктуры. Подобное положение исходит от восприятия самого явления кибербезопасности, определяемого специалистом, как совокупность мер по защите национального киберпространства, принимаемых государством как в виде реакционных мероприятий, так и виде превентивных мер, распространяющихся как на киберинфраструктуру, так и на окружающие её субъекты. В данном случае акцент производится на значимость человеческого ресурса, в качестве определяющего общее состояние кибербезопасности[[29]](#footnote-30).

В целом, позиции европейского экспертного сообщества основываются на принципе «soft security»[[30]](#footnote-31), основой которого выступают положения о необходимости проведения «ненавязчивых» превентивных мер по отсеиванию субъектов, потенциально способных выступить в качестве угрозы всей инфраструктуре. Таким образом, в очередной раз подчёркивается значимость человеческого фактора в состоянии кибербезопасности наших дней. В противовес данным суждениям выступает принцип «hard power», основным «проповедником» применения которого в киберпространстве на сегодняшний день выступает НАТО.

Организация Североатлантического договора, выделяемая в рамках данного исследования в качестве единого субъекта информационной среды, принимая в январе 2008 года Стратегию по киберобороне, в качестве реакционных мер, на ранее упомянутые события в Эстонии, где серьёзному удару подверглась киберинфраструктура государственных институтов[[31]](#footnote-32), охарактеризовала феномен кибербезопасности как совокупность принимаемых правительствами стран, международным сообществом и населением планеты, в частности, мер, направленных на защиту индивидуальных, общественных и государственных кибернетических систем, информации и информационных ресурсов, развитие национальных и международных механизмов борьбы с угрозами киберпространства[[32]](#footnote-33). Таким образом, определяющим положением восприятия кибербезопасности с точки зрения организации выступает необходимость учёта и построения эффективной системы контроля и регулирования киберсреды, фактически выступающей основным гарантом дееспособности феномена. При этом, следуя вышеупомянутому принципу «hard power», основными механизмами обеспечения безопасности в исследуемой области НАТО избирает привычные способы подавления вероятных угроз, не отрицая возможности проведения самостоятельных операций в киберпространстве, с целью уничтожения инфраструктурных компонентов, представляющих угрозу не только национальной безопасности государств-членов, но и международной кибербезопасности[[33]](#footnote-34). Элементы построения политики «hard power» организацией прослеживаются в действующей нормативно-правовой базе НАТО, где заложены основные принципы функционирования субъекта[[34]](#footnote-35).

В дополнение к вышесказанному, следует отметить, что объединённый центр передовых технологий киберобороны НАТО в заглавии своего официального интернет-портала, содержащего определения основных терминов связанных с киберпространством, отмечает, что позиция организации Североатлантического договора в отношении детерминирования самого киберпространства и принципиальных субъектов, действующих в нём, исходит из обобщения позиций, выраженных в нормативно-правовых актах государств-членов организации, а также учитывая нюансы, выработанные научным сообществом за последние десятилетия, что позволяет создать более успешную и прогрессивную систему киберобороны, охватывающую всю широту области кибернетической инфраструктуры[[35]](#footnote-36).

Тем ни менее, не смотря на все положительные стороны вышеупомянутых позиций зарубежных специалистов и международных организаций, в восприятии феномена с их стороны практически не уделяется внимание правовому аспекту проблематики и влиянию нормативно-правовой базы современности на развитие явления киберсреды. Чего нельзя сказать об отечественных экспертах в области безопасности, в какой-то мере обладающих инновационной позицией в отношении рассматриваемого феномена. Российская Федерация, её правительственные и научно-исследовательские институты, с момента формирования кибербезопасности и киберпространства в качестве полноценной области для ведения международной борьбы находятся на передних рубежах обороны киберсреды[[36]](#footnote-37), ежегодно выступая инициатором международного диалога в области необходимости выработки международных механизмов контроля и регулирования киберпространства о чём свидетельствует принятая Генеральной Ассамблеей Организации Объединённых Наций в ноябре 2015 года Резолюция России по кибербезопасности, предписывающая необходимость выработки чётких международных принципов и механизмов реагирования на вредоносные действия государственных и частных институтов в киберпространстве. Данная резолюция, в случае успешного сотрудничества ООН с экспертами в области кибербезопасности, способна стать базисом, той модели прогрессивного развития нормативно-правовой и технологической составляющих национальной и международной безопасности, которая несколько позже будет рассмотрена в исследовании.

Отмечая прогрессивность взглядов российского академического и военно-политического сообщества и обобщая выработанные ими суждения в отношении сущности киберпространства и кибербезопасности, формируется единая школа, отражающая современное состояние феномена и влияние на него факторов внешней и внутренней среды. Таким образом, с точки зрения отечественных специалистов, феномен кибербезопасности представляет из себя безопасность субъектов киберпространства, среды, включающей не только технические средства, но и совокупность операционного взаимодействия человека и программного обеспечения, а также телекоммуникационные сети, на просторах которых данная активность осуществляется, достигаемую прежде всего принятием совокупности мер по сохранению стабильности и правопорядка в электронной инфраструктуре, поддержанию дееспособности среды в целом, а также гарантирующих резистентность национальных и международных институтов, интегрированных в киберпространство, выраженных в виде формирования строгой нормативно-правовой, институциональной и технической базы. Другими словами, сущность феномена выражается в грамотном построении совокупности базовых элементов, гарантирующих стабильность информационных инфраструктур[[37]](#footnote-38)[[38]](#footnote-39)[[39]](#footnote-40)[[40]](#footnote-41). В качестве необходимой ремарки, которая в дальнейшем позволит избежать путаницы и возникновения определённых расхождений, стоит отметить, что в российской нормативно-правовой базе понятия кибербезопасности и киберпространства чаще подменяются терминами информационная безопасность и информационное пространство, сохраняя значение первых[[41]](#footnote-42)[[42]](#footnote-43).

Получается, что восприятие феномена кибербезопасности в разных уголках планеты напрямую связано выделением основополагающих субъектов киберпространства. К таким субъектам можно отнести и правовой фон, рассмотренный свыше как один из базовых элементов феномена кибербезопасности. Помимо того, наблюдаемые темпы технологического прогресса, заставляют научное сообщество задумать об эффективности применяемых методов обеспечения безопасности в киберпространстве. Одними из первых на совершенно иной путь восприятия киберсреды, как было отмечено свыше, встали российские академические круги, вплотную занявшие выработкой действенных правовых механизмов и их продвижение в массы. Какие успехи были достигнуты в данном направлении будет рассмотренное несколько позже. Однако, стоит отметить, что современная нормативно-правовая база Российской Федерации по обеспечению национальной безопасности в области киберпространства на настоящий момент является одной из наиболее прогрессивных в сравнении с зарубежными аналогами[[43]](#footnote-44).

**Основные угрозы информации и информационной инфраструктуре**

Формированию подобного восприятия кибербезопасности в разных частях планеты, помимо структурных компонентов феномена, в определённой мере способствовал анализ групп угроз, исходящих из киберпространства и воздействующих на него. В данном вопросе на современном этапе развития феномена международным сообществом также не найдено единой концепции. Наиболее остро в международном дискурсе о кибербезопасности стоит вопрос о полномочиях государственных институтов в киберпространстве: наглядно данную проблему демонстрирует различие политик «hard power» и «soft power», применяемых на западе, в НАТО, и на востоке, в Российской Федерации, в Китае и в некоторых государствах ближнего востока, соответственно. Основное различие состоит в принципах использования силовых ресурсов киберпространства за пределами национальных границ: воздействие на информационную инфраструктуру зарубежного государства для одних будет рассматриваться в виде оборонительных или же превентивных мер, а для других в виде неприемлемого акта агрессии[[44]](#footnote-45)[[45]](#footnote-46).

Наиболее полное представление о категориях деструктивных феноменов киберпространства в своей работе представил британский специалист П. Корниш, разделивший угрозы киберсреды на следующие категории[[46]](#footnote-47):

- Деятельность хакеров-одиночек

- Организованная преступность, действующая в глобальных интернет-сетях

- Идеологический и политический экстремизм

- Проводимая государством информационная агрессия

Данные группы вредоносных источников в том или ином виде находят отражение в работах большей части специалистов, уделяющих внимание данному направлению. Подобное разделение обусловлено характером и масштабами предполагаемого ущерба. Деятельность хакеров-одиночек, хоть и способна нанести колоссальный урон инфраструктуре государства, однако предполагает активность гениального специалиста в области киберпространства, в то время как подавляющее большинство подобных компьютерных гениев ещё с первого десятилетия XX века находятся под неустанным наблюдением национальных правительств и не изредка привлекается государственными институтами для модернизации собственного программного обеспечения и создания дополнительных рубежей киберобороны, о чём свидетельствует большое количество опубликованных документальных материалов.[[47]](#footnote-48)[[48]](#footnote-49) Помимо того, возможность привлечения подобного рода гражданских специалистов прописана в нормативно-правовой базе ряда национальных служб безопасности, а также в некоторых международных организациях, как, к примеру, в ни раз упомянутой организации Североатлантического договора[[49]](#footnote-50). Таким образом, деятельность одиночек прежде всего принято связывать с локальными проявлениями нарушения правопорядка в киберсреде, а потому они относятся к категории наименьших угроз кибербезопасности, даже в рамках одного государства[[50]](#footnote-51). Ярким примером активизации данной группы угроз можно обозначить инцидент от 14 августа 2014 года, когда атаке злоумышленника подвергся официальный twitter-аккаунт российского премьер-министра Дмитрия Анатольевича Медведева. В ходе разбирательства выяснилось, что хакер-одиночка опубликовал на странице известной социальной сети от имени политика ложное заявление о решении уйти в отставку. Реакция спецслужб последовала незамедлительно: через 30 минут сообщение было удалено, а в прессе было представлено опровержение, появившейся информации[[51]](#footnote-52). Таким образом, фактически государственная киберинфраструктура не пострадала, однако был наглядно продемонстрирован механизм пагубного использования киберпространства в личных целях. К более серьёзным последствиям от действий хакера-одиночки привели недавние события, имевшие место во время президентской гонки в Соединённых Штатах. Тогда злоумышленнику удалось проникнуть в компьютерную сеть Демократической партии государства и похитить из хранящихся в ней архивов данных определённый массив информации. Некоторые из заполученных незаконным путём документов позднее были опубликованы, нанеся определённый ущерб позициям демократов на предстоящих выборах[[52]](#footnote-53). В конечном счёте, данный пример также ярко обозначает существование определённой связи между инцидентом в киберпространстве и его последствиями в реальном мире, что подтверждает изначально выраженную позицию относительно роли высокой интеграции человека и общества в электронное пространство.

Следующей из представленных категорий угроз выступает деятельность групп хакеров, обозначенная как организованная преступность. Данный вид неправомерной активности в киберпространстве, пожалуй, является наиболее распространённым. Некоторые исследователи, ввиду повышенной опасности проявления подобной активности, а также масштабности последствий, к которым она может привести, соотносят данную категорию с понятием кибертерроризма. Впрочем, в академических кругах разных стран данный термин чаще используется в качестве демонстрации вероятной опасности, ввиду отсутствия на современном этапе инцидентов, имеющих ярко выраженный террористический характер[[53]](#footnote-54), чего не скажешь об организованной преступности. Неправомерные действия в кибернетическом пространства группы злоумышленников, как отмечалось свыше, встречаются на регулярной основе. Примером тому может служить 2013 год, насыщенный инцидентами данной категории: ноябрьский взлом интернет порталов правительства Сингапура, взлом аккаунтов Барака Обамы в социальных сетях Facebook и Twitter в октябре, сентябрьское проникновение хакеров в систему Министерства иностранных дел Бельгии, взлом и публикация ложных сведений на новостном портале РИА-Новости в мае того же года, глобальное снижение скорости передачи данных в европейском интернет-пространстве датированное мартом 2013 год[[54]](#footnote-55) - всё это и многие другие события стали результатом пагубного воздействия организованных групп хакеров, вылившегося в существенное ухудшение состояния киберпространства во всём мире. Все перечисленные события имели место в течении всего одного года, при том что были названы далеко не все самые масштабные инциденты, происходившие в киберсреде при участии группы злоумышленников. По этой причине, политика большинства стран в области киберпространства призывает национальные органы безопасности фокусировать основные усилия на контроле и регулировании данной группы вредоносных субъектов. В дополнение, хотелось бы отметить наиболее известные хакерские группировки, организации, выделяемые национальными и международными службами безопасности: Lizard Squad, Anonymous, LuizSec, Phantom Squad[[55]](#footnote-56).

Не меньшее количество дискуссий в рамках международного научного сообщества ведётся и насчёт идеологического и политического экстремизма в киберпространстве: основным поводом для споров в данном случае является вопрос о возможности сопоставления понятий экстремизма в сети и кибертерроризма[[56]](#footnote-57). Тем ни менее политически мотивированные неправомерные действия в киберпространстве до 2017 года считались редкостью. Зачастую схожие инциденты принято просто относить в категории государственной агрессии либо же организованной преступности. Однако данный феномен отчасти можно рассмотреть в инциденте, имевшем место в ноябре 2010 года: тогда упомянутая прежде группировка Anonimus совершила ряд кибератак на инфраструктуру международных компаний PayPal, Visa и других, мотивировав свои действия стремлением защитить ресурс WikiLeaks от нападки со стороны властей и международных корпораций[[57]](#footnote-58)[[58]](#footnote-59)[[59]](#footnote-60). Тем ни менее, даже этот пример, который хоть и имеет политическую подоплёку, скорее будет отнесён к организованной преступной деятельности. Впрочем, на интенсивности проявления подобного рода категории угроз способна сказаться тенденция, описанная в конце следующего параграфа и связанная с активизацией деятельности государственных институтов в киберпространстве. Что же касается идеологически мотивированной неправомерной деятельности, то более чётко, рассматриваемую группу правонарушений в киберсреде охарактеризовывает законодательная база Российской Федерации, в которой при перечислении основных угроз национальной безопасности упоминается воздействие террористических и экстремистских формирований с целью «нагнетания межнациональной и социальной напряжённости», осуществляемое с использованием технологий киберпространства[[60]](#footnote-61).

В поднятом ранее вопросе о характеристике воздействия государства на информационную инфраструктуру и о возможности появления пагубных последствий подобной активности, склонен возразить мнению некоторых специалистов о правомерности использования собственных силовых ресурсов киберпространства за рубежом[[61]](#footnote-62). Подобные действия также необходимо считать полноценной угрозой кибербезопасности. В данном случае за примерами далеко ходить не нужно: наглядной иллюстрацией вредоносного воздействия на киберинфраструктуру государственными институтами может послужить выявленный 12 мая 2017 года компьютерный вирус WannaCry, пострадавшими от которого только в первый день его активности считаются более 57 000 компьютеров и компьютерных систем по всему миру. На настоящий момент продолжается расследование произошедшего в киберпространстве инцидента, однако, предполагается, что причастным к разработке вредоносной программы, парализовавшей работу как частных лэптопов, так и крупных государственных учреждений по всему миру, включающих в себя больницы, системы телекоммуникаций и транспортного сообщения, может быть непосредственно Агенство национальной безопасности Соединённых Штатов, которое с момента подписания новой Стратегии киберобороны, в апреле 2015 года, вело разработку новых механизмов воздействия на киберпространство[[62]](#footnote-63)[[63]](#footnote-64). По первоначальным оценкам специалистов, наибольший ущерб был нанесён инфраструктуре Российской Федерации, Украины, Великобритании и части других европейских государств. Некоторые эксперты полагают, что данные действия могли быть мотивированны подозрениями американской стороны в причастности русских служб специального назначения к хакерским атакам, случившимся накануне выборов президента США. Таким образом, в случае подтверждения представленной информации на официальном уровне, будет продемонстрирована одна из первых крупномасштабных кибератак, подготовленных государственными институтами. Учитывая наличие передовых кибернетических ресурсов и весомой финансовой поддержки, предполагается, что действия государственных формирований в киберпространстве в ближайшие годы может перейти в ранг наиболее опасных угроз национальной кибербезопасности[[64]](#footnote-65), а потому будет требовать принятия новых интонационных мер по противодействию угрозам подобного характера, среди которых первостепенную значимость будет представлять именно нормативно-правовая основа кибербезопасности, сформированная на международном уровне.

Как уже отмечалось и было разобрано, каждая из вышеперечисленных групп угроз кибербезопасности обладает особым характером воздействия на киберинфраструктуру, а потому представляет опасность для отдельных направлений киберпространства в особенности. По этой причине следует подробнее разобрать по каким ведущим направления специальные государственные и частные формирования вырабатывают защитные механизмы с целью укрепления общего состояния безопасности в среде. Первостепенным направлением обеспечения стабильности киберпространства выступает защита интернета как такового. Как уже отмечалось ранее, данный феномен выступает основополагающим звеном функционирования всего киберпространства, поскольку формирует саму систему, объединяющую разобщённые технологии в единую информационно-кибернетическую сеть. Не менее значимым компонентом кибербезопасности выступает защита компьютеров, представляющих технологическую основу киберпространства. Защита данных - защита основного субъекта информационного пространства, безусловно, вытекает из совокупности других направлений ведения киберзащиты, тем ни менее экспертным сообществом принято выделять данной направление в отдельную категорию. Помимо того безопасность киберпространства формирует защита таких областей как: телекоммуникационная инфраструктура, каналы передачи данных, программного обеспечения и приложений, основных услуг[[65]](#footnote-66). Угроза одной из перечисленных жизненно-важных для функционирования киберсреды категорий может повлечь за собой деструктивные последствия во всей среде, приведя к парализации сети в целом. Ярким примером подобного пагубного влияния может послужить упомянутый ранее вирус WannaCry, основной эффект которого выражается в блокировке компьютерной системы и моментальном шифровании хранившихся на электронных носителях массивов информации. Сообщается, что распространение вируса в больницах и госпиталях Великобритании привело к тотальному отключению всех электронных систем учреждений, всвязи с чем подавляющее число пострадавших заведений было вынуждено прекратить приём новых пациентов и распустить большую часть персонала в виду отсутствия возможности продолжать проведение необходимых процедур[[66]](#footnote-67). В данном случае весьма чётко отражено воздействие краха одной из составляющих кибербезопасности, приведшее в недееспособности среды в целом: отключение компьютеров привело расформированию единой системы, сети здравоохранительных институтов.

Таким образом, большая часть государств мира, при построении собственной политики в отношении киберпространства основывается на анализе исходящих из кибернетического пространства угроз, выделении основных направлений их воздействия, а также на анализе современной технологической базы, что в совокупности позволяет выработать ряд прогрессивных мер по обеспечению кибербезопасности. На современном этапе, к приведённому перечню небезосновательно начинают припаивать нормативно-правовую базу, воздействие на киберсреду которой будет подробно рассмотрено позднее. Впрочем, даже сейчас можно с уверенностью отметить, что активизация категории угроз относящихся к проводимой государством информационной агрессии, напрямую связана с упущениями нормативно-правовой составляющей, поскольку на международном уровне на данный момент отсутствует какой-либо правовой механизм, способный препятствовать формированию вредоносных субъектов институционального уровня, то есть созданию органов превентивного воздействия на предполагаемую угрозу.

**Правовые аспекты вопроса**

Переходя к подробному рассмотрению правовых аспектов проблематики кибербезопасности, следует в очередной раз отметить, что сам феномен кибербезопасности сформировался на стыке тысячелетий, в некотором смысле потеснив с первых рядов существовавшие ранее понятия информационной безопасности, информационного противоборства, информационной агрессии и некоторых других устоявшихся явлений. Тем ни менее часть уже сформировавшейся к тому периоду нормативно-правовой базы унаследовала черты предшествующих феноменов, а доля определений перекачивала в современное национальное и международное законодательство и теперь непосредственно ассоциируется с понятием кибербезопасности[[67]](#footnote-68). Так, принятая в 2000 году Доктрина информационной безопасности Российской Федерации выступала в роли реакционных мер военно-политического руководства страны на зарождение феномена киберпространства, однако использованная в ней терминология в большей степени соответсвует феномену информационного пространства, несколько отличающегося от киберсреды, впрочем, адаптированная к современным реалиям.

В целом же, современная нормативно-правовая база в области кибербезопасности выступает совокупностью правовых актов, принятых как на государственном так и на международном уровнях, регулирующих субъекты киберпространства и направленных на поддержание стабильного функционирования инфраструктуры киберсреды[[68]](#footnote-69). Таким образом, чтобы раскрыть правовой аспект проблематики кибербезопасности, следует сосредоточить внимание на рассмотрении ведущих государственных и международных документов, выделяя особенности и совпадения в позициях государств, что в дальнейшем позволит выработать единый прогрессивный путь развития нормативно-правового поля на международном уровне.

Прежде всего, рассмотрим законодательные акты, принятые в Российской Федерации. Как уже отмечалось ранее, на протяжении долгих лет основополагающим документом, определяющим позиции военно-политического руководства страны в вопросах построения кибербезопасности, была принятая в сентябре 2000 года Доктрина информационной безопасности Российской Федерации. Обновлённая версия документа сохранила своё название и была подписана президентом РФ 5 декабря 2016 года. В тексте рассматриваемой доктрины содержатся «основные направления обеспечения информационной безопасности с учётом стратегических национальных приоритетов Российской Федерации»[[69]](#footnote-70). Среди основных интересов Российской Федерации в киберсреде выделяют положения о стремлении государства обеспечить возможность населению страны и государственным институтам беспрепятственно коммуницировать в электронном пространстве, обеспечить гарантии стабильности киберсреды, а также способствовать развитию национальной технологической базы. Помимо того, акцент производится на необходимости использования киберпространства в благих целях, что подтверждается пунктами «г» и «д» восьмой статьи Доктрины, в которых высшее военно-политическое руководство отразило намерение содействовать формированию международных институтов кибербезопасности для создания среды, в которой страны смогут осуществлять «равноправное стратегическое партнёрство»[[70]](#footnote-71). Одой из наиболее значимых характеристик основного субъекта киберпространства, информации, в принятом документе выделяется её достоверность. Таким образом, следуя выраженным в тексте Доктрины позициям Российской Федерации в отношении кибербезопасности, можно заключить, что рассматриваемый феномен на современном этапе развития государства выступает одним из наиболее важных для политического руководства направлений, которое напрямую связывается не только с областью обеспечения национальной безопасности страны, но и способно благоприятно воздействовать на экономику и развитие социально-общественных институтов. Наиболее значимым моментов выступает готовность и открытость высшего военно-политического руководства страны к ведению международного диалога.

Также в определении политического курса Российской Федерации в отношении феномена кибербезопасности одно из первостепенных значений играет последняя редакция Стратегии национальной безопасности Российской Федерации, подписанная Президентом страны 31 декабря 2015 года. Весьма значимым фактом является включение угроз исходящих из киберпространства в перечень основных угроз национальной безопасности страны. Тем ни менее, основные принципы, на которых будет основываться построение рубежей национальной обороны в киберпространстве, были в полной мере раскрыты лишь в вышеупомянутом документе.

Помимо Доктрины информационной безопасности и Стратегии национальной безопасности на территории Российской Федерации действует ещё один нормативно-правовой акт, в некотором смысле предопределивший появление вышеупомянутой Доктрины: указ Президента Российской Федерации за номером №1753 от 24.07.2013 «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». Данный документ относится к разряду элементов стратегического планирования[[71]](#footnote-72), а потому представляет большую ценность в рамках исследования перспектив развития феномена кибербезопасности. В отмеченном документе, как и в Доктрине информационной безопасности, рассматриваются основные пути прогрессивного развития феномена информационной безопасности, тем ни менее больший акцент производится на выделении конкретных механизмов регулирования среды. Так, одним из перспективных направлений виделось подписание конвенции информационной безопасности в рамках ООН, что в конечном счёте и было достигнуто с принятием Генеральной Ассамблеей Организации Объединённых Наций в ноябре 2015 года Резолюции России по кибербезопасности[[72]](#footnote-73). Однако, вопросы международной правовой среды будут рассмотрены несколько позже.

Соединённые Штаты, что вполне ожидаемо, играют наравне с Российской Федерацией довольно значимую роль в области кибербезопасности. Во многом подобное положение дел исходит от исторической подоплёки зарождения феномена интернета. Выступая в роли «создателей» электронного пространства, американское высшее военно-политическое руководство стремится занимать доминирующие позиции в области контроля, воздействия и распоряжения ресурсами киберпространства для чего регулярно совершенствует свою нормативно-правовую базу. Во главе угла современного правового аппарата обеспечения кибербезопасности в Соединённых Штатах стоит национальная Стратегия киберобороны принятая на вооружение руководством страны в апреле 2015 года. Исходя из пяти стратегических целей, представленных Министерством обороны страны в роли основополагающих механизмов реализации национальной безопасности государства в данной области, предельно чётко видно отсутствие интереса со стороны Пентагона к ведению международного диалога в области правомерного использования и контроля киберпространства. Подобный вывод основан на анализе положений Стратегии, в которой выделены следующие направления развития оборонительного и наступательного потенциала страны в электронном пространстве: развитие технологического потенциала страны, наряду с модернизацией вооружённых сил и выделением в них отдельных специализированных подразделений кибербезопасности; развитие единой системы Министерства обороны страны, повышение резистентности военной инфраструктуры; перераспределение обязанностей по контролю и регулированию национального киберпространства между государственными институтами; выработка наступательных, «превентивных», механизмов воздействия на киберпространство; развитие сотрудничества с союзниками и союзными организациями, такими как НАТО[[73]](#footnote-74).

Продолжая рассмотрение правового аспекта кибербезопасности в Соединённых Штатах Америки, следует обозначить ещё один не менее важный для формирования общей позиции государства документ, а именно Национальную политику кибербезопасности, подписанную высшим военно-политическим руководством страны в 2013 году. Стоит отметить, что позиции государства при сравнении двух вышеупомянутых законопроектов разительно отличаются друг от друга. Документ 2013 года прежде всего рассматривает вопросы формирования устойчивой национальной системы кибербезопасности и не предполагает, в отличие от акта 2015 года возможности проведения «экспансионистских» мероприятий в киберсреде[[74]](#footnote-75). Таким образом, ввиду сохранения силы обоих из перечисленных нормативно-правовых актов на современном этапе, предполагается, что руководство страны будет в большей степени придерживаться принципов изложенных в более позднем документе, а потому в отличие от позиций изложенных в нормативных документах Российской Федерации, американское правовое поле представляет киберпространство в виде непосредственной области противоборства, как отмечалось ранее, схожей с существующими полями сражений - наземными, воздушными и другими. Данный факт находит подтверждение в принятой в феврале 2015 года Стратегии национальной обороны США, в которой киберпространство отмечено как новая зона противоборства с государственными и негосударственными субъектами, а угрозы киберсреды выведены в ранг угроз национальной безопасности[[75]](#footnote-76).

Подобная позиция западного государства становится серьёзным барьером в вопросе выработки прогрессивных правовых механизмов в международной среде, особенно с учётом роли государства в Организации Объединённых Наций, представляемой экспертным сообществом в роли наиболее действенного рычага воздействия на международную среду[[76]](#footnote-77). Таким образом, на основании проведённого анализа сложившейся в государстве нормативно правовой базы формируется общая позиция страны в области кибербезопасности, постулаты которой в первую очередь ориентированы на национальные институты, от которых исходит как государственная так и международная безопасность. То есть основной упор в вопросе формирования действенных механизмов борьбы с киберугрозами делается на внутригосударственные институты, что в определённой мере способствует развитию и активизации последней группы угроз, именуемой государственными актами информационной агрессии в киберпространстве.

Рассмотрение национальных правовых аспектов кибербезопасности в любой исследовательской работе на данную проблематику не может обойтись без анализа феномена в рамках правового поля Китайской Народной Республики. В первую очередь данная тенденция мотивирована мировым соотношением количества пользователей интернет-пространства к региону мира. Так, в азиатской части планеты сосредоточено более 50% от общемирового количества интернет-пользователей[[77]](#footnote-78), что делает такие страны как Китай одними из основных субъектов киберпространства. Более того, особый интерес представляет специфика самого правового поля государства, приверженного некой изоляционистской политики в отношении киберпространства[[78]](#footnote-79). Исходя из нормативно-правовой базы государства, создание дополнительных слоёв безопасности национальной киберсреды, нередко приводящей к её изоляции от внешнего мира, прежде всего связано с отсечением пагубных элементов деструктивного характера от доступа в национальную кибернетическую систему. Особую роль в данном вопросе сыграла начатая с середины 90-х годов политика развития интернет-пространства. Первые нормативно-правовые акты ограничивающие воздействия внутренних субъектов на киберпространство страны были приняты на стыке тысячелетий, когда в 2000 году правительство страны ограничило национальных поставщиков интернет связи в области развития предоставляемых населению услуг и обязало их к получению лицензии на предоставление доступа в интернет-пространство. А в 2009 году вступил в силу ряд законопроектов ограничивавших в доступе более 100 тысяч интернет-порталов[[79]](#footnote-80).

Наиболее актуальными нормативно-правовыми документами Китайской Народной Республики, отражающим позиции государства в области обеспечения кибербезопасности, являются принятая 1 июня 2015 года Стратегия национальной безопасности и подписанная высушим военно-политическим руководством страны в декабре 2016 года Стратегия кибербезопасности. Из проведённого анализа данной группы источников следует, что оба из представленных свыше документов основываются на стремлении государства укрепить собственную систему кибербезопасности путём совершенствования институтов и технологической базы страны. Однако, Китай в тоже время отмечает готовность к выработке прогрессивных международных мер по контролю и регулированию международного киберпространства[[80]](#footnote-81). Таким образом, позиции Российской Федерации и Китайской Народной Республики предельно схожи в отношении необходимости принятия международных мер по противодействию угрозам киберсреды. По этой причине в последние несколько лет между государствами ведётся активный диалог по данному вопросу.

Выше были рассмотрены наиболее прогрессивные национальные правовые акты современности, принадлежащие странам, оказывающим решающее воздействие на состояние международного киберпространства. Безусловно, затронуть все существующие мировые законопроекты в рамках данного исследования является весьма трудновыполнимой задачей, особенно учитывая тот факт, что практически каждая страна на современном этапе своего развития уже обладает двумя, а то и тремя нормативными актами в арсенале своего правового поля. Поэтому, важнее будет рассмотреть не затронутый ранее феномен, носящий международный характер, однако исходящий из национальных законодательств стран. При анализе правовой среды нельзя не подчеркнуть значимость феномена конфиденциальности, который, к сожалению, в современном мире всё более теряет свой вес[[81]](#footnote-82): национальные правительства стран мира всё чаще прибегают к внутренним реформам в области права, затрагивающим вопрос свободы действий человека в интернет пространстве. Стремясь повысить контроль за киберпространством, в целях обеспечения национальной безопасности, принимаются законодательные акты, повышающие полномочия служб специального назначения в области сбора и анализа проходящих через киберинфраструктуру данных[[82]](#footnote-83). К подобного рода документам можно отнести: принятый в начале 2017 года «пакет Яровой», состоящий из двух законопроектов и обязующий телекоммуникационные институты хранить массив данных, передаваемый в голосовом, текстовом и иных возможных видах через электронное пространство, а также упрощающих процедуру использования данного массива органами безопасности; «Патриотический акт», принятый в Соединённых Штатах после событий 11 сентября 2001 года, фактически выступает олицетворением развеивания феномена конфиденциальности: документ предоставлял национальным органам безопасности широкие полномочия по сбору и анализу личных данных американских граждан, перемещающихся в электронном пространстве, что напрямую пересекалось с четвёртой статьёй конституции США и напряжении долгих лет критиковалось правозащитниками по всему миру. При этом, действие вышеупомянутого акта истекло лишь в 2015 году, когда президент страны Б. Обама, подписал «Акт о свободе», снявший часть полномочий служб безопасности беспрепятственно распоряжаться личной информацией американских граждан, однако оставив возможность для спецслужб запросить санкцию на получение необходимых им сведений. В конечном счёте, в качестве наиболее свежего примера размытия понятия конфиденциальность следует обратить внимание на подписанный 9 мая 2017 года указ Президента Российской Федерации, В.В. Путина, за номером №203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы». Данный нормативно-правовой акт выступает в поддержку принятого ранее «пакета Яровой», поскольку часть его статей посвящена механизмам поддержания общественной безопасности в сети интернет, путём исключения феномена анонимности из киберпространства[[83]](#footnote-84). Таким образом, получается, что национальная безопасность, как и кибербезопасность в некотором смысле идёт в противовес конфиденциальности, поскольку для её обеспечения правовой среде необходим доступ к личной информации пользователей.

Совокупность приведённых свыше документов в купе с конституцией и другими национальными правовыми актами государств составляет базовый уровень обороны страны. Невзирая на общую прогрессивность принимаемых национальных нормативно-правовых актов, существенных изменений в вопросе киберобороны за последние годы не наблюдается. Проблема современной кибербезопасности состоит в том, что киберпространство уже давно вышло за пределы одного государства и отныне носит транснациональный характер, что требует принятия международных мер. В доказательство данной гипотезе можно привести слова Министра внутренних дел Федеративной Республики Германии Томаса де Мезьер, которых утверждал, что «поскольку интернет не признаёт государственных границ, то и усилия по обеспечению его безопасности должны быть международными»[[84]](#footnote-85).

Таким образом, следующим шагом в рассмотрении правовых аспектов феномена кибербезопасности будет анализ действующих международных правовых норм и институтов. Однако, прежде чем преступить, стоит подчеркнуть, что рассмотренные свыше позиции трёх государств, выступающих одними из основных субъектов киберпространства, а именно кардинальные расхождения в восприятии прогрессивных механизмов развития феномена кибербезопасности, свидетельствуют о том, что на современном этапе международный диалог государств ведётся крайне медленно, а особые достижения наблюдаются исключительно в области двустороннего и группового сотрудничества[[85]](#footnote-86). Ярким примером последнего может послужить сотрудничество государств в вопросе кибербезопасности в рамках Организации Североатлантического договора. Впрочем, как отмечалось вначале исследования, подобные объединения рассматриваются как единый субъект киберпространства, а принимаемые в нём меры не могут быть расценены как меры полноценно международного характер. Более того, позиции данного формирования предельно схожи с проповедуемой Соединёнными Штатами политикой, а потому не представляет исключительного интереса.

Что же действительно заслуживает внимания, так это попытки государств принять международные меры по поддержанию кибербезопасности в рамках Организации Объединённых Наций, а также успехи достигнутые на данном пути. Одним из таковых как раз таки является переориентация деятельности Международного союза электросвязи в область регулирования международного киберпространства. Данной событие произошло в 2006 году, когда после проведения Всемирной встречи на высшем уровне по вопросам информационного общества, на приданный Организации Объединённых Наций союз были возложены функции по развитию и укреплению международного киберпространства и феномена кибербезопасности в частности. Результатом активности данной организации уже в первые годы её функционирования стало принятие в 2007 году Глобальной программы кибербезопасности. В статьях данного документа заложены основные принципы международного сотрудничества государств в области кибербезопасности, а именно, принятие правовых, технических и иных мер с целью создания потенциала киберпространства и продвижения международного диалога[[86]](#footnote-87). Тем ни менее, как показывает историческая ретроспектива, государства, выступающие основными субъектами международной кибербезопасности неохотно вступали в дискуссию и слабо стремились воздействовать на кибербезопасность международными механизмами. Однако, так продолжалось вплоть до 2014 года, до момента, когда технологический прогресс достиг таких высот, что некоторые государства уже не могли самостоятельно справляться с возникающими угрозами киберсреды. Поэтому с 2015 года проявляется высокая законодательная активность в различных регионах мира: одни страны, как Россия, Китай - на законодательном уровне закрепляют возможность и необходимость международного сотрудничества, в то время как другие, Америка, страны блока НАТО - полагаются на собственный или же групповой потенциал, будучи уверенными в собственной готовности устоять.

До наступления данного периода, когда мир затаился в ожидании активности одного из лидеров кибернетического пространства, в ООН был принят ряд документов, сформировавших определённое восприятие мировым сообществом проблем кибербезопасности. К таким документам можно отнести: резолюцию Генеральной Ассамблеи ООН по «Борьбе с преступным использованием информационных технологий» за номером 55/63 и 56/121 от 2001 и 2002 года соответственно, а также по «Созданию глобальной культуры кибербезопасности» за номером 57/239 от 2003 года. Также особую роль сыграли ежегодные доклады Генеральной Ассамблеи об «Использовании информационно-коммуникационных технологий в целях развития», в них содержались основные достижения международного сообщества в области укрепления киберпространства, а также отмечалось возникновение новых вызовов кибербезопасности.

На сегодняшний день одной из основных сохранившихся форм сотрудничества государств на международном уровне в области развития кибербезопасности выступает международный форум управления интернетом. В повестку данного мероприятия ежегодно выносятся насущные проблемы киберсреды, относящиеся как возникновению новых угроз кибербезопасности, так и к появлению передовых технологий защиты электронного пространства. Предполагается, что в рамках данной встречи, политическое руководство стран-участниц сможет договориться в вопросе принятия прогрессивных мер развития международной кибербезопасности, однако, единственной инициативой последних лет стала предложенная Российской Федерацией в ноябре 2015 года Резолюция о «Достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности», в которой содержался призыв государств-членов ООН продолжить совместную выработку прогрессивных механизмов сотрудничества и развития киберпространства.

Подводя итог анализу современного состояния кибербезопасности, следует отметить, что основополагающей проблемой феномена на международном уровне выступает не наличие большого количества внешних угроз, а состояние разрозненности взглядов отдельных государств, препятствующих не только выработке единой концепции восприятия феномена и эффективных механизмов противодействия возникающим угрозам, но и построению международного диалога, как такового. Тем ни менее стоит отметить, что на национальном уровне некоторые из рассмотренных государств добились больших успехов в построении национальной кибербезопасности. Как уже ни раз отмечалось, главенствующую роль в формировании феномена кибербезопасности играет совокупность нормативно-правовой и технологической базы. Причём подобная форма применима не только в границах одного государства, но и на международном уровне: обладая достаточно прогрессивной и постоянно развивающейся технологической базой, мировое сообщества нуждается в действенной правовой базе, а точнее в сопровождающем данное явление аппарате принуждения. Объяснить подобную необходимость довольно просто: из проведённого исследования было установлено, что основную угрозу для любого государства в киберпространстве представляют внешние субъекты, в то время как большинство локальных актов агрессии в киберсреде удаётся успешно ликвидировать до возникновения каких-либо широкомасштабных последствий. Подобная логика исходит из возможности государства применять превентивные меры исключительно на территории собственной юрисдикции, тогда как внешние угрозы обладают большим потенциалом и поражающей способностью ввиду отсутствия барьеров для совершения акта агрессии. Таким образом, создав определённую нормативно-правовую базу, венцом которой будет выступать международный институт, обладающий неким аппаратом принуждения, технологической и правовой базой для проведения международных операций в киберпространстве, удастся избежать проявления глобальных последствий влияния вредоносных субъектов на киберпространство. Впрочем, возвращаясь к характеристике современного состояния кибербезопасности, единственный вывод, который можно сделать на данном этапе исследования будет заключаться в фактическом отсутствии нормативно-правовой базы в её естественном понимании, о чем свидетельствует изложенная свыше модель незаменимости аппарата принуждения.

**ГЛАВА II. МЕТОДОЛОГИЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ КИБЕРБЕЗОПАСНОСТИ**

**Современные механизмы противодействия угрозам кибербезопасности**

Ранее были рассмотрены несколько факторов, формирующих феномен кибербезопасности, а именно технологическая и нормативно-правовая база. Каждый из перечисленных уровней формирует особые механизмы упреждения и реакции на возникшую угрозу кибернетической среды. Однако, помимо данных факторов, особым воздействием на формирование действенной системы кибербезопасности страны оказывают также экономические механизмы, определяемые научным сообществом в отдельную категорию[[87]](#footnote-88). Поэтому принято разделять методы противодействия угрозам кибербезопасности на несколько групп, анализ которых позволит выделить используемые на национальном и международном уровнях процедуры, способствующие повышению уровня устойчивости среды к основным угрозам кибербезопасности. Исходя из начальной позиции исследования, особый акцент будет уделён правовым методам, впрочем не останутся без внимания и технологические, а также экономические меры, при рассмотрении которых будут выделены передовые инструменты воздействия на киберпространство.

Итак, как уже ни раз было отмечено прежде, первостепенное значение в области противодействия угрозам кибербезопасности на современном этапе развития человечества уделяется именно нормативно-правовому уровню. При его доскональном анализе становится очевидным, что именно правовая база способствует развитию технологической составляющей и формирует экономические механизмы кибербезопасности, а значит, именно с принятия правовых норм создаются первые рубежи киберобороны. Подобная практика наиболее полно раскрывается при рассмотрении конкретных нормативно-правовых актов, формирующих государственные позиции в области кибербезопасности. Так, первые шаги по совершенствованию оборонительного потенциала Российской Федерации в киберсреде были приняты уже в 2000 году с подписанием Доктрины информационной безопасности. В данном документе содержатся шаги, последовательное выполнение которых позволит улучшить общее состояние информационной защищённости государства. Одним из наиболее значимых направлений в создании действенной системы обороны в принятом в начале столетия документе выделяется «формирование базы правового обеспечения информационной безопасности»[[88]](#footnote-89). Реализация данного курса предполагает создание и принятие ряда документов, способствующих развитию институциональной и технологической базы государства, осуществлению конкретных мероприятий по выработке механизмов защиты информации. На практике, реализация вышеупомянутых направлений прогрессивного развития сферы кибербезопасности выразилась в принятии таких документов как Закон «О государственной тайне», утверждённый высшим военным руководством страны в 1993 году, однако регулярно редактируемом, ввиду расширения области его применения, которой также отчасти является киберпространство.

Последние поправки в вышеупомянутый документ датируются мартом 2015 года и в первую очередь связаны с наблюдаемым техническим прогрессом в области электронной среды, приведшем к возникновению новых угроз информационной и кибербезопасности. Среди основных функций государства выделяются не только положения о классификации государственно-значимой информации, но и о распределении полномочий между национальными институтами, призванными препятствовать активизации угроз одному из наиболее значимых субъектов киберсреды - информации[[89]](#footnote-90). Одним из таких органов выступает утверждённая Указом Президента Российской Федерации от 2004 года Межведомственная комиссия по защите государственной тайны, в сферу ответственности которой входят функции по координации федеральных и региональных органов, имеющих доступ к государственной тайне, по выработке перечня сведений содержащих государственную тайну, а также, что наиболее важно, по определению размеров вероятного и реального ущерба, нанесённого вредоносными субъектами, также действующими и в киберсреде, в случае распространения засекреченных сведений[[90]](#footnote-91). Безусловно, были перечислены далеко не все функции рассматриваемого института, однако, даже упомянутого перечня достаточно, для формирования представления о текущем методе обеспечения кибербезопасности нормативно-правового характера.

Продолжая анализ нормативно-правовых актов в качестве механизма по поддержанию и совершенствованию национальной системы кибербезопасности, нельзя не рассмотреть Концепцию «государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утверждённую Президентом Российской Федерации в декабре 2014 года на основании выпущенного ранее Указа от 15.01.2013 о создании соответствующего института. Следуя положениям вышеуказанного документа, важно выделить, что создаваемый в результате его реализации аппарат на законодательном уровне наделяется полномочиями по прогнозированию, обнаружению и реакции на возникающие угрозы киберсреды, а также полномочиями по созданию необходимой для реализации предъявляемых задач материально-технической базы, путём организации и проведения исследований в области механизмов воздействия на киберпространство[[91]](#footnote-92). Таким образом, исходя из правовой базы, сам по себе сформировавшийся институт будет выступать первостепенным средством государственного воздействия на киберсреду, применяемым в целях поддержания и развития кибербезопасности.

Выше были рассмотрены нормативно-правовые методы, выступающие как превентивными, так и реакционными мерами на угрозы киберсреды. Подобная характеристика проводимых мероприятий исходит из тех функций, которые предписывает нормативно-правовая среда непосредственно документам, а также создаваемым в результате их реализации институтам. Основываясь на выделенной свыше Доктрине информационной безопасности, ставшей основой деятельности государственных и негосударственных институтов по созданию и развитию единой системы национальной кибербезопасности, можно чётко разделить методику воздействия на рассматриваемые категории. Так, к примеру, положения о необходимости создания и развития законодательной базы страны скорее будут выступать в качестве превентивных мер, в то время как статьи, предусматривающие выработку и принятие мер ответственности за правонарушения в киберсреде носят ярко выраженный реакционный характер. Подобная направленность отмечается не только в рассмотренной Доктрине, но и в большинстве других законодательных актов как Российской Федерации, так и других государств - субъектов киберпространства.

В предыдущем абзаце был поднят вопрос о выработке и принятии мер ответственности за правонарушения в киберсреде. Его рассмотрение позволит проанализировать не затронутый ранее механизм принуждения, карательный аппарат, формируемый государством в том числе в киберпространстве для поддержания безопасности как инфраструктуры, так и в субъектов кибернетической сети. Конституция Российской Федерации определяет права человека на неприкосновенность личной информации, а также на свободу связанной с ней деятельностью по хранению и использованию в информационной среде[[92]](#footnote-93), в то время как основополагающим документом в области наложения ответственности за совершённое правонарушение в киберпространстве в рамках законодательства Российской Федерации выступает Уголовный Кодекс РФ, в котором на современном этапе содержится порядка пятидесяти статей, посвящённых исключительной правонарушениям в киберпространстве, а также более 10 связанных с данной тематикой положений[[93]](#footnote-94). Помимо того, дополняют данный перечень и статьи «Кодекса Российской Федерации об административных правонарушениях», а также другие нормативно-правовые акты, как к примеру, Федеральный Закон «Об информации, информатизации и защите информации»[[94]](#footnote-95), принимаемые для расширения правовой базы. При этом, исходя из совокупности правовых документов, следует заключить, что под правонарушением в области киберпространства в современном правовом поле Российской Федерации понимаются совершённые или планируемые противоправные действия, идущие в нарушение действующего порядка и представляющие потенциальную или реальную угрозу киберсреде. В конечном счёте, совокупность нормативно-правовой базы государства в области правонарушений в киберпространстве, а так же её постоянная модификация с учётом развития феномена кибербезопасности, позволяет гарантировать стабильность и безукоризненность в работе судебных органов государства, выступающих олицетворением института принуждения. Необходимость закрепления подобного механизма на международном уровне подчёркивалась в предыдущих главах и будет подробно рассмотрена в последующих.

Продолжая рассмотрение методологии противодействия угрозам киберсреды и переходя к следующей группе мер, направленных на поддержание дееспособности, стабильности и развития национальной и международной кибербезопасности, рассмотрим категорию технологических механизмов воздействия на киберпространство. Данная категория является наиболее неустойчивой к воздействию внешних факторов, основным из которых выступает технологический прогресс, имеющий, как было отмечено ранее, перманентный характер. Исходя из подобной характеристики технологической базы как отдельно взятого феномена, напрашивается вывод о необходимости его регулярного развития, модификации и даже в некотором смысле эволюции, что на практике подтверждается чуть ли ни в каждом принятом документе, имеющем отношение к феномену кибербезопасности. Законодательная база государств мира в один голос отмечает необходимость развития научно-исследовательского потенциала, обязывая национальные институты регулярно работать над совершенствованием действующих и изобретением новых технологий, для обеспечения надлежащего уровня защищённости киберинфраструктуры[[95]](#footnote-96)[[96]](#footnote-97)[[97]](#footnote-98).

Требования, предъявляемые к национальной технологической базе могут существенно разниться в зависимости от рассматриваемого региона, однако наиболее концептуально полное отражение следует из анализа американской нормативно-правовой базы, требования в которой являются наиболее высокими в сравнении с мировыми стандартами, а потому способствуют формированию конкурентной системы кибербезопасности. Среди основных составных частей технологического потенциала высшее военно-политическое руководство страны рассматривает наличие технологий базовой, подсистемной защиты, функцией которой выступает предотвращение обнаружения внутренних систем и каналов связи за счёт подавления исходящих от них электромагнитных и радиосигналов. Также неотъемлемыми составляющими выделяются системы, обеспечивающие интернет- и компьютерную безопасность, которые обыденно представлены в виде антивирусного программного обеспечения, а также в виде устройств, фильтрующих входящий и исходящий сигнал и распределяющих его на внутреннюю и внешнюю сеть. Помимо того, безопасность киберинфраструктуры напрямую зависит от наличия у государства систем обнаружения, выявляющих незарегистрированный сигнал, и систем реагирования на изменения качественного характера киберпространства, автоматизированных на принятие мер по экстренному восстановлению исконных параметров сети[[98]](#footnote-99).

Перечисленные механизмы дают положительных результат, эффективно реагируя и противостоя угрозам, только в том случае, если работают в форме единой системы, организация которой является весьма непростой задачей, ввиду того, что за каждую из отмеченных систем в отдельности могут нести ответственность сразу несколько государственных институтов, обычно представленных органами безопасности страны[[99]](#footnote-100). Таким образом, формирование единой структуры лежит на плечах нормативно-правовой базы, обеспечивающей достаточное количество кадровых и аппаратных единиц, а также предписывающей механизмы их взаимодействия, повышая эффективность и оперативность предпринимаемых мер.

К сожалению, государственный научно-исследовательских аппарат весьма ограничен в специалистах, в следствие чего бывает не способен самостоятельно произвести необходимые технические и программные работы[[100]](#footnote-101). Поэтому, зачастую в вопросах обеспечения национальной безопасности привлекаются частные лица и негосударственные компании, обладающие необходимой военно-политическому руководству страны ресурсной базой, позволяющей развить оборонительный потенциал государства. В вопросе формирования технологической базы подобный опыт сотрудничества встречается постоянно, а наблюдения последних лет свидетельствуют о расширении перечня направлений, по которым ведётся технологический обмен[[101]](#footnote-102). К примеру, компании, разрабатывающие программное обеспечение, на регулярной основе предоставляют государственным институтам системы защиты от вредоносного программного обеспечения, воздействующего не только на персональные устройства, но и на компьютерную сеть в целом. Среди таких компаний наиболее известными и задействованными в сотрудничестве с многочисленными государствами считаются: Kaspersky, Eset, Sophos, Trend Mirco и некоторые другие. Также, повышению эффективности способствует использование передового электронно-вычислительного оборудования, которое в случае задействования частных международных или государственных компаний поставляется фирмами AMD и Intel[[102]](#footnote-103). Таким образом, видно, что сотрудничество в технологической области ведётся не только с национальными предприятиями, но и допускает использование зарубежных технологий. Поэтому, формирование технологической базы и её непосредственная эволюция зависит сразу от нескольких факторов и требует как развития национального научно-исследовательского потенциала, так и роста международного взаимодействия с государствами и компаниями. Однако, следует отметить, что данная тенденция не отражает позиции всех стран без исключения: наиболее яркое тому подтверждение наблюдается в принятой в конце 2016 года новой Доктрине информационной безопасности, в которой отмечается необходимость снижения зависимости государственных кибернетических систем безопасности от зарубежных технологий[[103]](#footnote-104).

На данном этапе анализа механизмов обеспечения кибербезопасности уже были разобраны такие элементы как технологические и правовые формы воздействия на национальное и международное киберпространство. Тем ни менее, как и в случае невозможности развития технологического потенциала без принятия соответствующих правовых норм, оба фактора теряют свой вес без присутствия определённой финансовой поддержки их реализации. Данную функцию берёт на себя выделенный в особую группу экономический фактор. Его основополагающей задачей выступает действенное регулирование финансовых потоков исходящих от государства. Перераспределение основных направлений финансовой поддержки позволяет ускорить темпы развития государственных институтов, способствует достижению прогресса в научно-исследовательской области, за счёт сосредоточения потоков на действительно нуждающихся в модернизации сферах, а также позволяет избежать нецелесообразного использования государственного бюджета. В конечном счёте, влияние экономического фактора на совокупность описанных сфер, напрямую связанных с кибербезопасностью, приводит к повышению эффективности государственного воздействия на киберпространство.

Ровно также как и с технологической базой, области воздействия экономического фактора регламентируются законом. По этой причине, для выявления сущности рассматриваемого механизма необходимо рассмотреть нормативно-правовую базу, формирующую его. Безусловно, основополагающим финансовым инструментом нормативно-правового характера любого государства является Бюджет страны, составляемый и принимаемый с целью эффективного распределения национальных ресурсов для реализации государственных потребностей. В соответствии с приводимой Федеральной службой государственной статистики информацией, расходы на обеспечение национальной безопасности в 2016 году составили чуть менее 7% от общегосударственных объёмов, что в национальной валюте составляет 2072,2 миллиарда рублей или 2,6% ВВП страны[[104]](#footnote-105). Значимая часть данных средств была выделена именно на развитие кибербезопасности, совершенствование институтов, а также на модернизацию технологической базы.

Основное влияние экономического фактора на развитие национальных технологий воздействия на киберпространство выражается в реализации статей бюджета, направленных на финансирование научно-исследовательских и опытно-конструкторских работ, именуемых НИОКР. В докладе федерального казначейства, отражённого в «Ежегодном мониторинге средств, выделенных из федерального бюджета на финансирование НИОКР» за 2016 год, отмечается, что финансирование фундаментальных и прикладных исследований в области технологий, направленных на обеспечение национальной безопасности Российской Федерации, за последние четыре года кардинальных количественных изменений не потерпело и составило 7% от общего числа выделенных из федерального бюджета на НИОКР средств, что в количественном эквиваленте составляет порядка 45 миллиардов рублей[[105]](#footnote-106). Важно отметить, что по данному показателю Российская Федерация располагается на 32 месте из 91 в международном рейтинге ЮНЕСКО, оценивающем уровень расходов стран мира на НИОКР[[106]](#footnote-107). Таким образом, на наглядном примере было разобрано влияние экономического фактора, действующего в совокупности с остальными механизмами, на общее состояние устойчивости киберпространства, а также на развитие системы кибербезопасности государства.

Таким образом, на основании грамотного применения совокупности рассмотренных свыше механизмов государство формирует эффективную систему противодействия угрозам киберсреды, основополагающим элементом которой выступает заложенная нормативно-правовая база. Впрочем, нельзя не отметить, что обозначенная эффективность достигается исключительно путём единовременного задействования всех трёх упомянутых механизмов, поскольку высокий уровень взаимозависимости элементов не позволяет им воздействовать на киберсреду в одиночку. Также немаловажным наблюдением стало выделение характера воздействия каждого из элементов на состояние кибербезопасности в целом: каждый из проанализированных механизмов может выступать в форме превентивных мер либо же в форме реакционных действий. И если в случае с правовым и технологическим механизмами всё предельно ясно, то экономический фактор, носящий преимущественно превентивный характер, обусловленный функциональными особенностями элемента, может быть оценен и в качестве реакционной меры, поскольку исходит из необходимости воздействовать на отстающую отрасль кибербезопасности.

**Будущее кибербезопасности в правовом поле**

Рассмотрение фундаментальных основ феномена кибербезопасности ни раз показывало, что первостепенную значимость в вопросе его формирования оказывало именно нормативно-правовое поле, которое благодаря подобной характеристике, как было выяснено, выступает первым рубежом обороны национального киберпространства. Тем ни менее вопросы национальной безопасности в сфере киберобороны напрямую зависят и от достижений международного сообщества в выработке действенных наднациональных механизмов контроля и регулирования международной киберсреды, современное состояние которых, не взирая на развитость национальных законодательств, разительно отстаёт от требуемого уровня[[107]](#footnote-108). Ввиду нарастающих противоречий государств, процесс построения конструктивного диалога из года в год замедлял свои темпы. Подобная тенденция, безусловно, не могла благоприятно сказаться на общем уровне защищённости международной киберсреды, от которой, как было отмечено прежде, со слов Министра внутренних дел Федеративной Республики Германии, зависит и уровень защищённости национальной киберинфраструктуры[[108]](#footnote-109). По этой причине далее будут рассмотрены возможные сценарии развития феномена кибербезопасности в правовом поле с учётом эволюции международной нормативно-правовой базы, как определяющего элемента в построении национальной политики в области обеспечения безопасности электронной среды.

Итак, выделим несколько сценариев развития международного диалога: первым, в какой-то степени утопичным сценарием, будет выступать возможное нахождение компромисса между политикой «hard power» и «soft power», применяемыми в большей степени на западе и на востоке, соответственно. В конфронтации данных идеологий основополагающее значение имеет приверженность запада позициям «национального превосходства», выступающего гарантией безопасности страны и предполагающего наличие сильных государственных институтов, способных не только самостоятельно отразить агрессию в киберпространстве, но и подавить возникновение потенциальной угрозы, посредством применения превентивных механизмов воздействия за рубежом[[109]](#footnote-110). По этой причине, создание международных институтов, обладающих возможностями контроля киберпространства, идёт в противовес национальным интересам западных государств, поскольку предполагает невозможность задействования национальных структур без санкций со стороны вышестоящих международных органов. По мнению экспертного сообщества, подобный образ мышления является весьма прогрессивным с точки зрения достижения национальных интересов, однако не помогает построению международного сотрудничества, в свою очередь способного искоренить некоторые категории угроз кибербезопасности, не нанося вред киберинфраструктуре государств[[110]](#footnote-111).

В данном случае возможность преодоления существующих разногласий зависит исключительно от желания и возможности стран, придерживающихся политики «hard power», к которым в первую очередь относятся государства-члены Организации Североатлантического договора, страны блока НАТО, пойти на уступки мировому сообществу. Подобный шаг маловероятен, однако всё же возможен, и на его принятие способно повлиять сразу несколько факторов. Во-первых, толчком к развитию международного диалога может послужить смена позиций высшего военно-политического руководства Соединённых Штатов Америки, выступающих опорой вышеупомянутой Организации. Подобная переориентация может быть вызвана инцидентом, в котором национальная система обороны просто напросто будет неспособна противостоять внешней или даже внутренней угрозе, которая в конечном счёте приведёт к весомым последствиям для киберинфраструктуры Соединённых Штатов и их союзников. В таком случае правительства рассматриваемых государств будут вынуждены поддержать мировое сообщество в вопросе необходимости создания международных механизмов по противодействию агрессии в киберпространстве. Однако, данный вариант развития событий всё же носит весьма субъективный характер, а потому не гарантирует достижения прогресса. Тем ни менее, сохраняется и возможность реализации сценария, при котором уступки западных государств будут минимальными, а потому шанс его осуществления куда более вероятен нежели у рассмотренной ранее перспективы. Компромисс в данном случае будет базироваться на выдвижение инициативы о создании международного органа, основанного на принципах Совета Безопасности Организации Объединённых Наций, в котором решающее значение имеет вопрос распределения полномочий между его членами. Таким образом, реализация подобного проекта возможна даже в рамках действующего Совета Безопасности, однако, в таком случае требуется существенное реформирование нормативно-правовой базы, с целью выработки общеприемлемых принципов восприятия феномена кибербезопасности, киберугроз и связанных с ними понятий, что на современном этапе выступает одной из основных проблем в вопросе международного регулирования киберпространства.

Изменения подобного характера в области международной кибербезопасности не могут ни отразиться на развитие нормативно-правового поля. Прежде всего качественным изменениям подвергнется международное право, в котором, по всей вероятности, наконец, появятся нормативно-правые акты, чётко определяющие феномен кибербезопасности и близкие к нему понятия, такие как киберпространство, киберинфраструктура и киберагрессия, что несомненно упростит задачу противодействия вредоносным элементам среды. Более того, велика вероятность возникновения принципиально нового международного института, наделённого правовой базой функциями контролирующего органа, способного эффективно воздействовать на возникающую агрессию, применять санкции в отношении вредоносных субъектов, а также способствовать повышению среднемирового уровня научно-технологического развития, предъявляя к странам определённые требования по совершенствованию данной базы. Совокупность изменений на международном уровне приведёт к развитию межгосударственного диалога во всех направлениях, что в том числе отразится на открытости и готовности государств к сотрудничеству в принципиально новых сферах. К примеру, технологическая зависимость, воспринимаемая современными государствами в качестве влияющего на общее состояние кибербезопасности негативного фактора, перейдёт в раздел способствующих экономическому и социально-культурному развитию факторов, поскольку будут снижены риски использования подобных технологий в пагубных целях государствами-производителями. Что же касается непосредственно национального законодательства стран, то особо заметным будет смещение акцента в область международного сотрудничества и необходимости дальнейшего развития международных механизмов противодействия угрозам киберсреды. Также принципиальным изменениям подвергнутся основные направления, обеспечивающие национальную кибербезопасность, так, к примеру, вопросы государственной агрессии в киберсреде отойдут на второй план, поскольку определённая доля ответственности за данный сектор перейдёт на международный орган, в то время как вопросы борьбы с недостоверной информацией и её распространением зарубежными средствами массовой информации, а также вопросы контртеррористической деятельности выйдут на первый план, ввиду того, что международный институт будет не способен обеспечить государственную защищённость в этих областях.

Рассмотренные свыше перспективы носят сравнительно благоприятных характер, прежде всего для международного диалога, благодаря которому в конечном счёте могут быть сформированы прогрессивные механизмы международного контроля и воздействия на киберпространство, а значит может быть повышен уровень как международной, так и национальной защищённости от угроз киберсреды. Тем ни менее, учитывая современные тенденции, при которых нахождение обозначенного компромисса становится фактически невозможным, нельзя не затронуть более пессимистичную модель развития, при которой интенсивность построения диалога останется на наблюдаемом нынче невысоком уровне, если вовсе не снизится, а единственным международным органом, напрямую связанным с феноменом киберпространства останется не отличающийся высоким уровнем эффективности Международный союз электросвязи.

Подобная перспектива будет способствовать отстранению государств от общемирового курса и переориентации национальной нормативно-правовой базы на индивидуальный путь развития систем кибербезопасности, предполагающий необходимость совершенствования всех трёх ранее упомянутых механизмов воздействия на киберпространство, для того, чтобы они могли самостоятельно противостоять возникающим угрозам киберсреды. Также, меньше внимания и ресурсов будет выделено на международное сотрудничество, ввиду утверждения несостоятельности и неэффективности данного механизма. Национальное киберпространство в ущерб эффективности будет тотально переходить на государственную технологическую базу, уровень которой во многих областях ниже зарубежных аналогов. Помимо того, восприятие феномена кибербезопасности государствами мира будет основываться на исключительных позициях стран в отношении трактования связанных с ним явлений, а потому способно выразиться в появлении большего количества противоречий и конфликтных областей между государствами. Таким образом, изменения приобретут, а точнее уже отчасти приобрели принципиально обратный характер[[111]](#footnote-112). Совокупность последствий развития данного более пессимистичного сценария приведёт к нарастанию международной напряжённости не только в киберсреде, но и за её приделами, что рано или поздно будет способствовать переходу кибервойны в реальные боевые действия.

Подводя итог как проведённому анализу перспектив развития правового сегмента кибербезопасности, так и методологии противодействия угрозам киберсреды в целом, следует заключить, что состояние национальной кибербезопасности находится в прямой зависимости от уровня международного сотрудничества государства в данной области. Таким образом, на современном этапе государства мира стремятся обеспечить максимальный уровень национальной защищённости разрабатывая стратегии наиболее эффективного применения трёх основных методов воздействия на киберпространство: нормативно-правового, технологического, а также экономического. Их совокупность позволяет создавать в государстве эффективную систему кибербезопасности, способную в случае необходимости оказать сопротивление агрессии в киберпространстве, гарантировав тем самым устойчивое функционирование национальной киберинфраструктуры.

Что же касается непосредственно нормативно-правового поля, то его роль в вопросе формирования единой системы киберобороны переоценить невозможно: развитие любого другого механизма воздействия, а также киберинфраструктуры в целом напрямую связано с успешным нормативно-правовым регулированием, устраняющим административные барьеры, возникающие в ходе изменения общенационального курса.

**ГЛАВА III. КИБЕРБЕЗОПАСНОСТЬ КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Состояние и уровень информационной защищённости Российской Федерации**

Проведённый анализ фундаментальных основ феномена кибербезопасности показал, что на формирование системы национальной безопасности в области киберпространства оказывает влияние сразу несколько внешних и внутренних факторов, не последнее место среди которых занимают угрозы, исходящие из киберсреды. Поражающий фактор данных угроз способен оказывать колоссальное влияние не только на функциональные способности электронной инфраструктуры, но и ввиду высокого уровня интеграции государства и его институтов в выделяемое пространство, наносить повреждения деструктивного характера в целом системе национальной безопасности. По этой причине подавляющее большинство стран выделяют кибербезопасность в качестве неотъемлемой составляющей безопасности государства. В их число входит и Российская Федерация, нормативно-правовая база которой прямо указывает на зависимость государственных и общественных институтов от современных технологий[[112]](#footnote-113), а потому требует проявления повышенного внимания к киберинфраструктуре, как жизненно необходимого для обеспечения дееспособности государства элемента.

Отмеченную свыше зависимость наглядно демонстрируют статистические данные, приведённые в новой Стратегии развития информационного общества, принятой 9 мая 2017 года. Исходя из указанных в документе показателей, количество интернет-пользователей отечественного сегмента сети за 2016 год составило более 80 миллионов человек[[113]](#footnote-114), что в процентном соотношении с общим населением страны на конец года составляет порядка 55% граждан, хотя бы единожды воспользовавшихся электронным ресурсом. Подобные цифры говорят о высоком уровне информатизации общества, состояния при котором одной из основных потребностей человека выступает необходимость наличия свободного доступа к информационным ресурсам[[114]](#footnote-115). Однако, социальная сфера является не единственным направлением в Российской Федерации, в котором современные технологии занимают одну из первостепенных позиций по своей значимость, а также востребованности. Из экономической статистики, отражённой в вышеупомянутой Стратегии, известно, что более 2,3% от общего ВВП страны проходит через национальные кибернетические сети. Данные показатели обладают явной тенденцией к росту, что послужило мотивом для отражения в действующей нормативно-правовой базе положений, свидетельствующих о стремлении высшего руководства страны развивать на территории государства цифровую экономику, вид «хозяйственной деятельности, в котором ключевым фактором производства являются данные в цифровом виде, обработка больших объёмов и использование результата анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг»[[115]](#footnote-116). Дабы придать картине законченный вид, стоит рассмотреть и сферу государственного управления, а точнее область взаимодействия государственных институтов с населением. С открытия в 2009 году Портала государственных услуг Российской Федерации его пользователями стали более 34 миллионов человек[[116]](#footnote-117). Подобный способ взаимодействия государства и общества серьёзным образом облегчил бюрократические тяготы, а также способствовал повышению эффективности и качества предоставляемых услуг.

Существование рассмотренных элементов стало возможным благодаря взаимодействию государственных и общественных институтов с использованием современных технологий, современного киберпространства. По этой причине, угрозы киберинфраструктуре и возможность нарушения её стабильности идёт не просто в разрез национальным интересам Российской Федерации, но и выступает существенной угрозой функционированию государственных институтов, а значит является непосредственной угрозой национальной безопасности. Следуя данной логике, можно проследить чёткую взаимозависимость феномена национальной безопасности и феномена кибербезопасности, на современном этапе выступающего одним из основных элементов построения государственной системы безопасности.

Переходя от вопроса соотношения феномена кибербезопасности и явления национальной безопасности к рассмотрению современной обстановки в сфере киберпространства Российской Федерации, произведём непосредственную оценку состояния и уровня информационной защищённости государства, которая предполагает анализ эффективности реализации основополагающих факторов, формирующих феномен кибербезопасности, а именно: уровня развития нормативно-правовой, технологической и экономической базы, а также влияющих на них факторов, выраженных в виде национальных интересов, угроз национальной безопасности и других побочных явлений.

Прежде всего отметим основные угрозы национальной кибербезопасности, выделяемые нормативно-правовой базой Российской Федерации на современном этапе: следуя текущим общемировым тенденциям, стоит отметить, что грамотное применение информационных технологий способствует ускорению прогресса практически во всех областях функционирования государства, однако, в то же время, данный факт способствует возникновению новых угроз национальной безопасности, ввиду увеличения зависимости государственных и общественных институтов от кибернетической среды. По этой причине, в некоторых государствах наблюдается пагубная тенденция к выработке принципиально новых механизмов воздействия на государство, осуществляемое через киберпространство. Среди подобных механизмов можно выделить деятельность служб специального назначения в области оказания психологического воздействия, носящего деструктивный характер, на население страны. Помимо того, активизируются механизмы искажения и фальсификации информации в зарубежных СМИ, стремящихся оказать воздействие на государственные институты и общественное мнение, путём предоставления заведомо ложных сведений[[117]](#footnote-118).

В соответствии с последней редакцией Доктрины информационной безопасности, ещё одним вредоносным явлением, выступающим угрозой национальной безопасности Российской Федерации сегодняшних дней, исходящей из киберпространства, можно считать деятельность террористических и экстремистских формирований, направленную на разобщение нации, а также нагнетание внутриобщественной напряжённости. В тоже время не последнюю значимость имеет и развитие международной компьютерной преступности, зачастую оказывающей особое влияние на экономику государства, напрямую воздействуя на его финансовые институты[[118]](#footnote-119). Таким образом, комплекс перечисленных угроз национальной кибербезопасности формирует ряд вызовов, успешное преодоление которых гарантирует безопасность киберинфраструктуры и зависит от эффективности применяемых военно-политическим руководством страны превентивных и реакционных мер. Однако, прежде чем приступить к их рассмотрению выделим особенности современного состояния информационной защищённости Российской Федерации.

В области обороноспособности государства, решающим фактором нестабильности выступает использование отдельными государствами передовых технологий с целью достижения национальных интересов. Методы их реализации носят деструктивный характер, а потому зачастую противоречат нормам международного права и могут быть расценены как акт агрессии, угрожающий не только национальной, но и международной стабильности и безопасности. Опускаясь на уровень ниже и переходя к рассмотрению государственных и общественных институтов с точки зрения состояния их защищённости, следует отметить, что в данном случае основным внешним дестабилизирующим фактором воздействия будут выступать качественно преобразовавшиеся и приобретшие массовый характер кибератаки на информационную инфраструктуру. В свою очередь, низкий уровень научно-технического потенциала в Российской Федерации на современном этапе приводит к проявлению определённой зависимости технологической базы страны от зарубежных разработок, что, безусловно, негативно влияет на состояние защищённости экономической среды. Отмеченный прежде научно-технический потенциал также оказывает определённый уровень воздействия и на сферу развития науки, существенно снижая эффективность и темпы реализации научных разработок. И последним, но не менее значимым для общей характеристики уровня национальной безопасности элементом является показатель степени стратегической стабильности на мировой арене, способствующий развитию международного диалога в области формирования нормативно-правовых механизмов поддержания международной кибербезопасности, однако, находящегося под пагубным влиянием со стороны государств, стремящихся к занятию доминирующих позиций в мировой киберсреде[[119]](#footnote-120).

Итак, рассмотрев современное состояние основных отраслей обеспечения национальной безопасности и основные факторы, оказывающие особое влияние на каждую из сфер в отдельности, а также указав основные угрозы кибербезопасности государства, перейдём непосредственно к оценке эффективности применяемых национальными институтами мер по противодействию угрозам, исходящим из киберсреды. Рассмотрим обозначенные механизмы по порядку и в первую очередь заострим внимание нормативно-правовом механизме.

Уже ни раз отмечалось, что нормативно-правовая база Российской Федерации, выступая одной из наиболее передовых правовых систем, «идёт в ногу со временем», постоянно обновляясь и подстраиваясь под изменяемую конъюнктуру. В доказательство этому стоит обратить внимание на принятую в декабре 2016 года Доктрину информационной безопасности. Данный документ стал своевременной реакцией высшего военно-политического руководства страны на возникновение угроз принципиально нового характера, исходящих из киберпространства и заключающихся в активизации у зарубежных государств механизмов пагубного воздействия на киберсреду. Более того, с принятием 9 мая 2017 года Стратегии развития информационного общества, было уяснено большинство положений Доктрины, а сама Стратегия стала логичным продолжением политики начатой в декабре месяце. Нельзя не отметить также того факта, что в очереди на подписание стоит очередной нормативно-правовой акт именуемый Стратегическим прогнозом Российской Федерации, принятие проекта которого намечено на первые месяцы лета. Таким образом, формирование действенных механизмов по нормативно-правовому регулированию киберпространства в Российской Федерации исходит из принятия целого комплекса правовых актов, способствующих выработке действенной базы для развития государственных институтов, а также позволяет создать благоприятную основу для построение экономической и технической базы. Подобная модель развития, безусловно, является более прогрессивной нежели принятие самостоятельных нормативно-правовых документов, поскольку позволяет избежать гораздо больших административных барьеров, а потому способствует повышению эффективности принимаемых мер.

Следующим механизмом, выступающим, пожалуй, наиболее слабым из трёх звеньев, обеспечивающих должный уровень защищённости киберпространства в Российской Федерации, является технологическая база государства. Из анализа принимаемых в стране нормативно-правовых актов предельно чётко выделяется существующая проблема высокого уровня зависимости отечественной киберинфраструктуры от зарубежных технологий. Подобная зависимость, как отмечалось прежде, носит весьма пагубный характер, не позволяя отечественной системе национальной безопасности считаться самодостаточной. По этой причине, руководством страны был предпринят ряд мер по повышению научно-технического потенциала государства, однако, современное положение рассматриваемого механизма говорит далеко не в пользу прогрессивности существующей технической базы.

И, наконец, экономическая составляющая обеспечения национальной безопасности страны. На данном этапе весьма сложно высказать определённую позицию в отношении реализации экономических мер: проводимая ранее политика привела к положению, описанному свыше, в котором страна фактически не способна гарантировать безопасность своих институтов и киберпространства исключительно за счёт национальных средств. Тем ни менее, в данном направлении был предпринят ряд прогрессивных мер, позволивших переосмыслить и реорганизовать направления, по которым должна вестись основная финансово-политическая поддержка. Моментальных результатов от подобных изменений ждать не приходится: выделяемые задачи по повышению научно-технического потенциала страны и реорганизации её основных институтов, относящиеся к области непосредственной ответственности экономических механизмов, являются задачами далеко не краткосрочной перспективы. Поэтому, характеризуя уровень эффективности реализации механизмов экономического воздействия, на современном этапе скорее будет дана отрицательная оценка, ввиду наблюдаемого эффекта влияния политики прошлых лет, неэффективно использовавшей имеющиеся механизмы финансовой стимуляции государственных отраслей.

Немаловажной составляющей в анализе состояния и уровня информационной защищённости государства также является сравнительная характеристика данных показателей с аналогичными в других регионах мира. Подобное положение, прежде всего, исходит из озвученной ранее возможности применения ресурсов, предназначенных для защиты, в целях нападения. По этой причине стоит обратить внимание на несколько субъектов мирового киберпространства, представляющих особый интерес в данной связи, а именно, на Соединённые Штаты Америки, Европейский Союз, НАТО, а также Китайскую Народную Республику. Подобный анализ составляет не только определённую ценность в вопросе формирования единой и точной картины, отражающей положение дел в Российской Федерации, но и напрямую способствует выработке прогрессивной модели развития кибербезопасности, учитывая позиции основных субъектов киберсреды.

Прежде всего, начнём с рассмотрения нормативно-правовой составляющей. В данном вопросе львиная доля законодательной базы субъектов была рассмотрена ранее, в рамках изучения правового аспекта кибербезопасности, где, в частности, были отражены позиции Соединённых Штатов, НАТО и Китайской Народной Республики. В целом, охарактеризовать уровень реализации механизма правового воздействия в перечисленных свыше странах и формированиях можно достаточно высоко: свидетельством тому выступает наличие ряда нормативных актов, отражающих единую позицию и взгляды высшего военно-политического руководства на методы координирования киберпространства[[120]](#footnote-121)[[121]](#footnote-122). Большая часть данной нормативно-правовой базы была принята сравнительно недавно, что также выступает гарантом её актуальности. Таким образом, совокупность отражённых характеристик свидетельствует о том, что в данной области, сторонние субъекты киберпространства ничуть не уступают Российской Федерации. Тем ни менее, за рамками исследования до сих пор оставался Европейский Союз, положение которого на сегодняшний день оценить весьма непросто. С одной стороны, в ЕС сохраняет силу принятая 7 февраля 2013 года Стратегия кибербезопасности, выступающая основополагающим документом в области регулирования киберпространства и отражающая намерение государств-членов Союза создавать открытое, надёжное и безопасное электронное пространство по принципу «soft power»[[122]](#footnote-123). А с другой, часть государств Союза также входят в вышеупомянутую Организацию Североатлантического договора, исходя из чего образовывается явный конфликт в выделяемых интересах, победу в котором одерживает НАТО. По этой причине, имеющаяся законодательная база Европейского Союза отчасти несостоятельна, а потому, по мнению некоторых экспертов, носит более рекомендательный, нежели обязательный к исполнению характер[[123]](#footnote-124). Так, получается, что нормативно-правовая составляющая кибербезопасности Европейского Союза напрямую зависит от НАТО, тем ни менее, если рассматривать данный субъект в отдельности, можно заключить, что европейская правовая база нуждается в серьёзной доработке и обновлении, с целью создания единой системы кибербезопасности, которой на современном этапе фактически нет, а потому ЕС не может идти в сравнение рассмотренным прежде субъектам, по крайней мере в области правового регулирования феномена.

Ещё одной неотъемлемой составляющей в сравнении современного уровня защищённости киберсреды в разных регионах мира является технологическая база, а точнее её развитость. В данном направлении из обозначенных субъектов Российская Федерация занимает наиболее низку позицию, о чём свидетельствует опубликованный в августе 2016 года Глобальный инновационный индекс, в котором Российская Федерация располагается на 43 месте, сильно отставая от Китая, положение которого также невысоко[[124]](#footnote-125). Помимо того, во внимание следует принять обозначенный ранее рейтинг ЮНЕСКО по уровню расходов государств на НИОКР, в котором эти две страны также находятся довольно низко – 32 и 21 места соответственно[[125]](#footnote-126). Что же касается остальных рассматриваемых субъектов, то большая часть государств, которыми они представлены, располагаются гораздо выше в упомянутых списках, а потому по факту обладают более конкурентоспособной технологической базой и технологическим потенциалом. Таким образом, в данном аспекте отстающими можно считать Китай и Россию. Первая страна хоть и превосходит Российскую Федерацию в большинстве направлений, однако, не обладает достаточным технологическим фундаментом для построения независимой системы кибербезопасности.

И последней, однако не менее значимой составляющей защищённости государства, как было отмечено, выступает экономический фактор. В данном направлении гораздо более успешным субъектом является Европейский Союз, аккумулировавший усилия государств-членов на создание наиболее действенных экономических механизмов, которые не в последнюю очередь воздействуют на кибербезопасность государств и формирования в целом. В случае с Соединёнными Штатами, НАТО и Китайской Народной Республикой трудно выбелить основные недостатки экономических механизмов, по этой причине оценка прежде всего будет строиться на соотношении экономического и технологического факторов, как это было при анализе состояния и уровня защищённости российской кибернетической среды, поскольку именно развитие технологической базы указывает на грамотность использованных экономических ресурсов. Таким образом, КНР выступает наиболее слабым звеном данного перечня, обладая невысокими показателями научно-исследовательского потенциала. Что же касается финансовой составляющей в её прямом значении, то Российская Федерация по сравнению с остальными субъектами также обладает наименьшим количеством средств, которые можно дополнительно использовать на развитие сторонних отраслей, в том числе системы кибербезопасности. Данное заключение строится на основании соотношения Валового внутреннего продукта анализируемых стран, выступающего одним из основных показателей для сравнения экономик государств[[126]](#footnote-127).

Получается, что на сегодняшний день наиболее действенной системой кибербезопасности обладают Соединённые Штаты, в которых основные механизмы воздействия на киберпространство находятся на достаточно высоком для автономного функционирования уровне. Затем следует Организация Североатлантического договора, негативный эффект в которой оказывают обозначенные свыше расхождения в интересах отдельных стран Евросоюза. Однако, данный эффект более сказывается непосредственно на Европейском Союзе, основная проблема которого заключается в построении нормативно-правовой базы с учётом интересов всех государств-членов. И уже потом идут Российская Федерация и КНР, которые обладают схожими проблемами, а потому состояние и уровень защищённости киберпространства данных государств примерно одинаковые.

Таким образом, подводя итоги рассмотрению современного состояния кибербезопасности и уровня защищённости государственной киберинфраструктуры Российской Федерации, следует заключить, что совокупность рассмотренных факторов, влияющих на текущее положение дел в области гарантии национальной безопасности, а также выявленный уровень эффективности реализации механизмов воздействия на национальное киберпространство, вкупе с общемировыми тенденциями, формирующими актуальные угрозы национальной безопасности в киберсреде, и уровнем развитости зарубежных систем кибербезопасности - все вышеперечисленные факторы свидетельствуют, что современная национальная безопасность, даже с учётом предпринятых за последний год прогрессивных мер по повышению уровня защищённости, находится под непосредственной угрозой вредоносного воздействия со стороны как внешних, так и внутренних субъектов национальной киберсреды, и не способна эффективно противостоять агрессии на киберинфраструктуру со стороны более подготовленных и технически превосходящих акторов среды. Подобная характеристика нашла отражение в майских событиях текущего года, когда наблюдалась активизация вредоносного вируса WannaCry, наибольшие повреждения от которого, не смотря на общемировой характер последствий, были нанесены инфраструктуре Российской Федерации, Украины, Китая и Великобритании. Общий эффект от воздействия кибератаки сказался более чем на 200 тысячах компьютерных устройств в более чем в 150 странах мира. Основную угрозу данный вирус представляет для устаревшего, а потому и менее защищённого программного обеспечения, наличие которого в мировом соотношении как раз таки преобладает в инфраструктурных элементах обозначенных стран[[127]](#footnote-128). Таким образом, наглядно демонстрируется уровень развития отечественной технологической базы, выступающей одним из основных элементов слабости национальной системы киберобороны. Весьма показательным фактом также является то, что наиболее серьёзный ущерб государственным институтам на территории Российской Федерации был нанесёт Министерству внутренних дел страны, органу уровень защищённости кибернетических сетей которого должен выступать образцовым, однако, по всей видимости, таковым не является.

**Отечественное законодательство во взаимодействии с международным правом**

В данной части исследования будет рассмотрено несколько сценариев развития национального нормативно-правового поля, находящегося в определённой обратной зависимости от международного, а также непосредственно влияющего на формирование и эволюцию рассматриваемого феномена кибербезопасности. С учётом последних мировых тенденций будет сконструирована модель перспективного развития национальной законодательной базы, соответствующая позициям российской политической элиты в области обороны киберпространства и отражающая современные национальные интересы. Существенное влияние на формирование вышеупомянутой модели будет исходить со стороны действующих национальных, зарубежных, а также международных нормативно-правовых актов. Выведенный образец прогрессивного развития кибербезопасности и связанных с феноменом институтов, в конечном счёте может стать отображением перспективы развития российского правового поля и его влияния на явление кибербезопасности.

Наиболее актуальное отражение позиций военно-политического руководства страны зафиксировано в принятой 9 и опубликованной 10 мая Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы. В комплексе с утверждённой в декабре 2016 года национальной Доктриной информационной безопасности, документы формируют передовые направления развития киберсреды, официально зафиксированные в нормативно-правовой базе Российской Федерации[[128]](#footnote-129). Принятие вышеупомянутых правовых актов стало результатом воздействия совокупности внешних и внутренних факторов, прежде всего выраженных в интенсификации темпов мирового научно-технического прогресса, нарастанию напряжённости в области воздействия на киберпространство государственными и негосударственными акторами, а также активизации национальной политики государств, направленной на достижение доминирования в киберсреде. Стоит отметить, что под влиянием перечисленных факторов начатая в конце 2016 года политика перехода на «собственные рельсы в киберпространстве» окончательно утвердилась с принятием вышеупомянутой Стратегии, в которой фактически признаётся необходимость принятия самостоятельных мер, ввиду отсутствия перспектив с построением международных правовых механизмов регулирования взаимоотношений стран в киберпространстве[[129]](#footnote-130).

Подобная смена курсов мотивированна нарастанием напряжённости в международной киберсреде, выраженной в череде заявлений правительств, политических деятелей и национальных служб безопасности о зарубежном посягательстве на государственное кибернетическое пространство с возможным причинением ущерба инфраструктуре и национальной безопасности в целом[[130]](#footnote-131). Наблюдаемый отход от политики международного сотрудничества позволяет констатировать, что существовавшие споры о двух вероятных сценариях развития международной нормативно-правовой базы теряют свою актуальность после подписания Президентом Российской Федерации, страны, выступавшей одним из основных инициаторов международного диалога, указа о вступлении в силу документа, в котором говорится о необходимости усиления национальных механизмов воздействия на киберпространство, ввиду повышающейся угрозы возникновения агрессии в киберсреде, способной перерасти в полноценное противостояние, к которому отечественная инфраструктура должна быть готова.

Таким образом, обозначив основной курс развития, заявленный нормативно-правовой базой Российской Федерации, приступим к построению модели прогрессивного развития национальной системы кибербезопасности и отметим области, совершенствование которых имеет первостепенную значимость для достижения положительного результата. Одним из основных направлений, по которым должно осуществлять активное государственное нормативно-правовое регулирование, станет развитие национального научно-исследовательского комплекса. Отмечается, что необходимость принятия подобных мер исходит из потребности в избавлении от пагубной зависимости от зарубежных технологий и программного обеспечения, составляющих значимую часть технологической базы России на современном этапе. Отрицательный характер подобной зависимости прежде всего выражается в возможности зарубежных компаний влиять на национальную систему безопасности, путём неправомерного использования обозначенных технологий. По этой причине, для поддержания должного уровня защищённости отечественной киберинфраструктуры будет предпринят ряд мер по активизации научно-исследовательских работ в области создания конкурентноспособной и независимой технологической базы. К таким мерам можно отнести: установление нормативно-правовых ограничений на использование зарубежных технологий в инфраструктуре государственных и частных институтов; реорганизация экономических механизмов, ответственных за эффективное финансирование НИОКР; установление единой системы государственного контроля и мониторинга функционирования информационных комплексов обработки и передачи данных; создание единой обновлённой системы сертификации, используемых в киберпространстве технологий; создание благоприятной для ведения научно-исследовательской работы обстановки, посредством размещения справедливой площадки для построения конкурентноспособного предпринимательства среди отечественных разработчиков технологий и программного обеспечения. Некоторые из вышеперечисленных мер, регулируемых правовым полем, уже нашли отражение в отечественных нормативно-правовых актах, что лишний раз подчёркивает решительную уверенность военно-политического руководства в принятии мер по снижению уровня пагубной зависимости в технологической области.

Помимо технологической составляющей, гарантирующей безопасность государства, важную роль в формировании эффективной системы киберобороны будет играть противодействие распространению заведомо ложной, а также секретной информации, дискриминирующей государственные и частные институты, а также негативно влияющей на образ государства за рубежом[[131]](#footnote-132). Необходимость достижения высокого уровня защищённости достоверной информации аргументирована особой ролью обозначенного ресурса в современном мире, за счёт которого в большей степени формируются позиции как высшего военно-политического руководства страны, так и общественное мнение. Данный фактор в дальнейшем способен крайне негативно сказаться на взаимодействии Российской Федерации не только с западными государствами, но и со стратегическими партнёрами. Потому, в ходе достижения данной стратегически важной задачи, руководством страны будут задействованы нормативно-правовые механизмы, направленные на создание правовой и технологической базы, способствующей распространению исключительно объективной и безопасной информации. Выполнению отмеченной свыше задачи будет непосредственно способствовать принятие следующих мер: формирование надёжных каналов передачи и систем обработки информации, за счёт активизации отечественной технологической базы; развитие правовых механизмов контроля активности средств массовой информации; проведение культурных и образовательных мероприятий, направленных на развитие правосознания населения; совершенствование правовых механизмов лимитации доступа к засекреченной и не подлежащей распространению информации; создание платформы для успешного продвижения отечественной культуры и научных достижений за пределами Российской Федерации. Комплекс описанных мер будет определённым образом способствовать не только сохранению достоверности распространяемой информации, но и позволит укрепить общегосударственную систему регулирования потоков информации, не допускающую возникновения деструктивных элементов информационной среды.

Построение единой действенной системы кибербезопасности также зависит от уровня доступности информационно-технологических ресурсов во всех частях государства. По этой причине, сохраняющееся технологическое отставание некоторых провинциальных районов российских субъектов, выраженное в банальном отсутствии доступа к сети интернет, препятствует формированию законченной системы национальной безопасности[[132]](#footnote-133). Отмеченный свыше пагубный эффект особенно заметен в российских реалиях, где для эффективного и, что более важно, своевременного руководства и взаимодействия с территориальными единицами необходимо наличие средств моментальной передачи данных, выступающих основой кибернетических сетей. Получается, что совершенствование системы национальной безопасности помимо всего прочего также зависит от реализации нормативно-правовых мер по распространению современных информационных технологий в труднодоступные районы страны, для чего государственными институтами предпринимаются следующие меры: создание государственных программ стратегического значения по развитию и распространению доступа к сети интернет на территории Российской Федерации; организация мероприятий технического характера по совершенствованию и расширению сетей электросвязи; формирование нормативно-правовой платформы, предполагающей реализацию намеченных задач за счёт отечественных технологий и программного обеспечения. Реализация выделенных мер по распространению информационных ресурсов на ровне с перечисленными ранее направлениями будет выступать значимым элементом создания единой системы кибербезопасности государства, а потому является неотъемлемой частью модели прогрессивного развития киберпространства Российской Федерации.

Прежде, при рассмотрении феномена зависимости национальной технологической базы от оборудования и услуг зарубежных компаний, отмечалось, что его формированию способствовала нехватка кадровых ресурсов в государственных органах и частных предприятиях, способных самостоятельно устранять последствия воздействия на национальную киберинфраструктуру вредоносных субъектов киберсреды. Данный факт свидетельствует о необходимости развития не только научно-технического потенциала государства, но и о важности принятия мер по повышению уровня грамотности населения, особенно в области освоения современных технологий. К наиболее прогрессивным из них можно отнести: создание нормативно-правовой базы по контролю качества обучения в специализированных учебных заведениях; создание платформы для самореализации специалистов в области современных технологий; введение государственных программ по бюджетному финансированию образовательных программ рассматриваемого сектора; введение государственных программ по обязательному распределению выпускников специализированных учебных заведений с целью их задействования на стратегически значимых объектах киберинфраструктуры Российской Федерации. Сочетание успешной реализации каждой из озвученных мер в отдельности будет иметь благоприятный эффект не только на расширение кадрового резерва специалистов в области передовых технологий, но и, безусловно, будет способствовать наращиванию научно-технического потенциала государства, реализуемого за счёт возникновения большого числа специалистов, заинтересованных в создании инновационно-прорывных технологий и программного обеспечения.

Важно отметить, что национальная кибербезопасность и её обеспечение являют невозможными без осуществления государственного контроля киберпространства, выражаемого прежде всего в сборе и анализе стратегически важных сведений информационной среды. Подобный механизм воздействия напрямую затрагивает ранее рассмотренное понятие конфиденциальности, поскольку предполагает взаимодействие с личной информацией пользователей киберпространства. По этой причине одной из основных задач высшего военно-политического руководства страны, а также национальных служб безопасности является построение действенных механизмов и алгоритмов сбора и анализа сведений, основных на соблюдении необходимого баланса в области применения средств обработки данных и гарантией конституционных прав граждан на сохранение семейной и личной тайны[[133]](#footnote-134). Реализации упомянутой задачи будут способствовать как нормативно-правовые, так и технические меры, гармоничное сочетание которых позволит достичь требуемого результата без посягательство на права граждан. К числу прогрессивных мер, реализуемых в данной области, можно отнести: совершенствование нормативно-правовой базы, обуславливающей применение спецслужбами технологий по сбору и анализу информационных ресурсов на законных основаниях; проведение технологических мероприятий по модернизации алгоритмов сбора и анализа информации; выработка как нормативно-правовой, так и технологической базы по препятствованию незаконной обработке данных пользователей национальной киберсети; выработка правовой основы обеспечения государственного контроля за процессом сбора и анализа сведений, предаваемых в киберпространстве; нормативно и технологически обеспечить процесс обработки информации с использование сертифицированных отечественных технологий и серверов.

В конечном счёте, даже при условии отступления от международного курса развития кибербезопасности с целью создания собственной прогрессивной системы противодействия угрозам киберпространства, в политику государства в отношении развития исследуемого феномена закладываются механизмы поддержания международного диалога, хотя бы на минимально возможном уровне. Задействование подобных механизмов в первую очередь характеризуется: инициированием построения нормативно-правовой базы, не допускающей использования интернета в военных целях; инициированием построения нормативно-правовой базы, направленной на регулирование международной киберсреды с целью сохранения стабильности международной киберинфраструктуры; способствование интеграции отечественных стандартов сертификации технологий, задействованных в киберпространстве. Подобные инициативы редко встречают всеобъемлющую международную поддержку, однако являются неотъемлемой составляющей прогрессивного подхода к обеспечению кибербезопасности. Необходимость сохранения международных контактов в данном вопросе исходит из описанной ранее характеристики индивидуальной модели развития кибербезопасности, которая непосредственно способствует нарастанию международной напряжённости.

Таким образом, совокупность рассмотренных мер нормативно-правового характера, реализуемых или планируемых к осуществлению на территории Российской Федерации, как отмечалось прежде, направлена на создание независимой и резистентной системы национальной безопасности, акцент в которой будет осуществлён на формировании действенных национальных механизмов воздействия на кибернетическое пространство, с целью защиты населения Российской Федерации от угроз кибернетического характера. На современном этапе на стадии рассмотрения находится Проект стратегического прогноза Российской Федерации. Выступая основой для принятия реакционных мер на различные события в стране и за рубежом, документ мог бы стать дополнительной опорой при формировании модели прогрессивного развития феномена кибербезопасности в стране. Однако, вероятнее всего, выстроенная на основании действующей законодательной базы Российской Федерации перспектива кардинальным изменениям с принятием вышеупомянутого документа не подвергнется, поскольку существующая правовая основа данного сегмента национальной безопасности является не только наиболее актуальной, но и одной из самых передовых в мире. Убедиться в этом позволит доклад Секретаря Совета Безопасности Российской Федерации Президенту страны о «состоянии национальной безопасности и мерах по её укреплению», предписанный в качестве ежегодной меры по поддержанию и контролю реализации поставленных высшим военно-политическим руководством страны целей и задач, отражающих национальные интересы Российской Федерации[[134]](#footnote-135).

**ЗАКЛЮЧЕНИЕ**

Прогресс не стоит на месте. С этих слов начиналось исследование, ими же оно и закончится. За то время, которое было уделено созданию данной работы в мире произошло с десяток значимых событий, тем или иным образом связанных с феноменом кибербезопасности. Часть из них была рассмотрена в рамках описания характерных особенностей явления киберпространства и связанных с ним современных тенденций, а часть так и осталась за кулисами изложенного материала. Тем ни менее, на данном этапе, вероятнее всего, мало у кого остались сомнения в отношении нарастающей зависимости общества от электронной среды, а вместе с тем и о необходимости создания определённой системы безопасности, способствующей сохранению одного из наиболее важных ресурсов современности в руках его законного обладателя. Безусловно, речь идёт об информации и о том, что её защита в XXI веке имеет первостепенное значение для всего человечества. Порой, мы даже меньше боимся потерять свой персональный компьютер или же смартфон нежели утратить содержащуюся на данных устройствах информацию, которая приобрела материальную стоимость, сопоставимую с любыми другими окружающими нас вещами материального мира.

С момента становления информации, как основополагающего фактора мирового развития, появились и сопутствующие данному явлению угрозы, а там где есть угрозы - есть и феномен безопасности. Таким образом, ход человеческого развития сам по себе закрепил за понятием кибербезопасности характеристику неотъемлемого элемента общественного бытия. Как было выяснено, на современном этапе феномен стал означать нечто большее, нежели процесс защиты информации и ресурсов её хранения. Решающее значение в вопросе его восприятия стали играть внешние и внутренние субъекты киберсреды, оказывающие непрерывное воздействие на формирование явления как такового. Одним из основных факторов воздействия на рассматриваемый феномен кибербезопасности стало окружающее его нормативно-правовое поле, фактически создающее образ и характерные черты явления. Однако, способно ли данное поле эффективно воздействовать на киберсреду и на феномен кибербезопасности, в частности? И как человечеству может быть подвластен контроль за неосязаемым кибернетическим пространством, если зачастую оно не может управлять даже видимыми вещами? Подобная дилемма стала основной мотивацией к проведению более глубокого изучения правовых аспектов обеспечения кибербезопасности.

Первым этапом на пути разрешения сложившейся дилеммы стал анализ сущности киберпространства и отражение его восприятия в различных уголках планеты. Историческая ретроспектива позволила выделить процесс эволюции феномена интернета, ставшего основой для формирования кибернетического пространства, а также отчасти обосновать позиции некоторых сторон в вопросе оценки явления кибербезопасности. В целом, исходя из совокупности взглядов мирового сообщества, кибербезопасность определяется комплексом реализуемых мер, принимаемых как на государственном, так и на международном уровнях с целью достижения стабильности и защищённости кибернетического пространства и перемещающейся в нём информации, а также развития прогрессивных механизмов противодействия угрозам киберсреды. Однако, существенное отличие в точках зрения сторон, в каком-то смысле разделившихся на два лагеря, состоит в вопросе необходимости применения привычных методов подавления угроз в кибернетическом пространстве, предполагающих возможность проведения полноценных операций в киберпространстве. Подобная политика получила название «hard power» и выступила в противовес более гуманной политике «soft power». Расхождения во взглядах этих «лагерей» в конечном счёте выступили основным барьером для развития международного диалога и выработки действенных международных механизмов по противодействию угрозам, исходящим из кибернетического пространства.

Что же касается позиций российского высшего военно-политического руководства, а также экспертного сообщества в вопросе восприятия феномена кибербезопасности, стоит отметить, что за годы существования и развития явления в стране сформировалась одна из наиболее сильных школ оценки киберпространства, его элементов и близких к феномену субъектов. Характерной особенностью данной школы стало единообразие в трактовании фундаментальных основ проблематики, что благоприятно отразилось на становлении нормативно-правовой базы страны. Так, исходя из принятой в декабре 2016 года Доктрины информационной безопасности Российской Федерации, феномен определяется как «состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[[135]](#footnote-136). Приведённое свыше определение не только включает в себя отмеченную в самом начале работы позицию, выраженную в Концепции стратегии кибербезопасности Российской Федерации от 2013 года, но и качественно дополняет её, что даёт возможность сделать вывод о том, что на основании сформировавшейся школы регулярно ведётся исследовательская работа, направленная на обновление и развитие существующей понятийной базы, способствующей формированию основных и побочных элементов кибербезопасности страны, трактованию угроз национальной безопасности, а также выстраиванию прогрессивных механизмов противодействия. Таким образом, прогрессивность взглядов российских политических деятелей и экспертов в данном направлении становится одной из наиболее сильных сторон отечественной системы кибербезопасности, способной не только составить конкуренцию на мировом уровне, но и послужить основой для развития международной понятийной и нормативно-правовой базы.

Следующим шагом на обозначенном пути стало выявление современных угроз национальной и международной кибербезопасности, как первостепенного фактора пагубного воздействующим на киберпространство и киберинфраструктуру. Особую роль в их формировании сыграл стоящий во главе угла технологический прогресс, предоставляющий злоумышленникам всё более совершенные механизмы воздействия на киберпространство. В конечном счёте было выявлено четыре основных группы угроз национальной и международной кибербезопасности: деятельность хакеров-одиночек; организованная преступность; идеологический и политический экстремизм; проводимая государством информационная агрессия. На современном этапе больше всего себя проявили угрозы, носящие характер организованной преступности, однако наибольшая опасность, отмечаемая мировым экспертным сообществом, исходит от последней из перечисленных категорий угроз, от активизации проводимой государствами информационной агрессии. Подобная опасность принципиально нового характера должна была бы способствовать построению конструктивного международного диалога, однако, стремление части государств занять доминирующие позиции в киберпространстве, основываясь на принципах рассмотренной свыше политики, предполагающей принятие подобных мер в качестве единственно возможного гаранта национальной безопасности, были весьма неоднозначно восприняты мировым сообществом, что вынудило большое количество государств перейти на национальный путь построения кибербезопасности.

Поскольку ранее была произведена оценка основных угроз кибербезопасности на современном этапе, нельзя было не рассмотреть основные методы противодействия им. Так, было выявлено, что принимаемые на государственном и международном уровнях меры по воздействию на киберпространство с целью укрепления стабильности и резистентности его институтов, а также киберинфраструктуры, можно разделить на следующие группы: нормативно-правовые, технологические и экономические. Подобное разделение содержится в большинстве нормативно-правовых актов государств мира, в том числе Российской Федерации, Соединённых Штатов, Южно-Африканской Республики и некоторых других государств-субъектов кибернетического пространства. Ни раз отмечалось, что первостепенное значение среди перечисленных механизмов прогрессивного воздействия будут носить меры именно нормативно-правового характера, выступающие инициирующим звеном любого процесса развития. Впрочем, значимым наблюдением стал и вывод о том, что эффективность в области применения данных методов достигается исключительно путём единовременного задействования всех трёх упомянутых механизмов, поскольку высокий уровень взаимозависимости элементов не позволяет им воздействовать на киберсреду в одиночку.

Раннее был упомянут переход части государств к построению системы национальной кибербезопасности, национальной киберобороны, ввиду нарастания напряжённости в кибернетическом пространстве, а также ввиду отсутствия развития международного диалога в области создания действенных механизмов контроля и совершенствования киберпространства, однако подобный сценарий в случае его перехода в ранг мировой тенденции будет исключительно способствовать нарастанию противоречий и в конечном счёте выльется из конфликта в киберпространстве в реальные боевые действия. По этой причине были также рассмотрены более благоприятные альтернативные сценарии развития событий, основанные прежде всего на необходимости построения международной нормативно-правовой базы, способной эффективно координировать взаимодействия государств на мировой арене. Достижение подобной перспективы возможно исключительно на основании нахождения компромисса между представителями «hard power» и «soft power». Обозначенные в основной части работы варианты хоть отчасти и являются утопичными, однако, в случае достижения даже минимального прогресса в обозначенных направлениях, откроются новые области для возможного международного сотрудничества.

В конечном счёте, после проведения достаточно подробного анализа фундаментальных основ феномена кибербезопасности, а также рассмотрения перспектив его развития в международном правовом поле, с учётом влияния всесторонних факторов, был сделан акцент на практической реализации рассмотренных механизмов нормативно-правового воздействия на кибернетическое пространство в реалиях законодательной базы Российской Федерации. Предварительным шагом в данном направлении стал анализ современного состояния и уровня информационной защищённости государства. Исходя из действующей нормативно-правовой базы было сделано несколько значимых выводов относительно восприятия феномена кибербезопасности высшим военно-политическим руководством страны. Одним из которых стало заключение о непосредственной зависимости понятия национальной безопасности от феномена кибербезопасности, на современном этапе выступающего одним из основных элементов безопасности государства.

В завершающей части исследовательской работы была выдвинута модель прогрессивного развития национальной системы безопасности, отражающая не только особенности реализации общепринятых механизмов воздействия на кибернетическую среду с учётом национальных и региональных особенностей, но и влияние на данный процесс общемировых тенденций и угроз кибербезопасности. За основу для построения данной модели были взяты позиции высшего военно-политического руководства страны, зафиксированные в принятой в декабре 2016 года Доктрине информационной безопасности Российской Федерации, а также в Стратегии развития информационного общества, утверждённой указом Президента Российской Федерации 9 мая 2017 года. Исходя из сформулированного прогноза, основным направлением развития отечественной нормативно-правовой базы станет переориентация внимания государственных и общественных институтов на слаборазвитые области кибернетического пространства, к которым в первую очередь относится научно-технический потенциал страны. Так, планируется активизация основополагающих для системы кибербезопасности страны механизмов c целью: развития научно-исследовательского комплекса, противодействия распространению заведомо ложной, а также секретной информации, повышения уровня доступности информационно-технологических ресурсов, устранения нехватки кадровых ресурсов, совершенствования средств сбора и анализа сведений информационной среды, поддержания международного диалога. Комплекс отмеченных направлений в совокупности призван повысить уровень защищённости кибернетической среды и её инфраструктуры, выступая наиболее прогрессивной мерой по совершенствованию кибербезопасности страны, чему прежде всего будет способствовать нормативно-правовая база государства, предписывающая национальным институтам обязательность выполнения намеченного комплекса.

Подводя общий итог исследованию правовых аспектов обеспечения кибербезопасности, в качестве основного приоритета национальной безопасности Российской Федерации, следует заключить, что правовое поле является наиболее эффективным механизмом противодействия угрозам кибернетической среды, поскольку способно оказывать не только реакционное, но и превентивное воздействие. Подобное свойство закона в совокупности с внешними факторами, влияющими на национальную безопасность Российской Федерации, оказали решающее влияние на позиции российского военно-политического руководства в вопросе выбора приоритетного инструмента для защиты государства, его интересов и инфраструктуры. Помимо того, нельзя не отметить, что, не взирая на ярко выраженный переход на «национальные рельсы» в вопросе построения действенной системы кибербезопасности, позиция российского военно-политического руководства будет основываться на двух направлениях: построение эффективной национальной нормативно-правовой базы и поиск возможностей для построения международного правового поля. При этом, в ближайшие годы акцент будет производиться исключительно на развитие государственных систем безопасности и их подготовке к отражению возможной агрессии в киберсети. Тем ни менее, специфика феномена кибернетического пространства заключается в его трансграничности, а потому обеспечение безопасности национальной в будущем будет напрямую зависеть от наличия действенных наднациональных институтов контроля и регулирования киберпространства.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ**

**Источники**

1. Конституция Российской Федерации от 12 декабря 1993 г. // Собрание законодательства Российской Федерации. - 2014. №31. - Ст. 4398
2. Закон Российской Федерации №5485-1 от 21 июля 1993 г. «О государственной тайне» // Собрание законодательства Российской Федерации. - 1997. №41.
3. Федеральный закон №172-ФЗ от 28 июня 2014 г. «О стратегическом планировании в Российской Федерации» // Собрание законодательства Российской Федерации. - 2014. №26. - Ст. 3378
4. Кодекс Российской Федерации № 195-ФЗ от 30 декабря 2001 г. «Об административных правонарушениях» // Собрание законодательства Российской Федерации. - 2002. №1. - Ст. 1
5. Кодекс Российской Федерации № 63-ФЗ от 13 июня 1996 г. «Уголовный кодекс Российской Федерации»
6. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074
7. Указ Президента Российской Федерации № 203 от 9 мая 2017 г. «О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»
8. Указ Президента Российской Федерации № 683 от 31 декабря 2015 г. «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №1. - Ст. 212
9. Указ Президента Российской Федерации № 1286 от 06 октября 2004 г. «Вопросы Межведомственной комиссии по защите государственной тайны» // Собрание законодательства Российской Федерации. - 2004. №41. - Ст. 4024
10. Указ Президента Российской Федерации № 803 от 03 февраля 2012 г. «Об утверждении Основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации»
11. Приказ Президента Российской Федерации № Пр-1895 от 07 февраля 2008 г. «Об утверждении Стратегии развития информационного общества в Российской Федерации»
12. Приказ Президента Российской Федерации № Пр-212 от 07 сентября 2000 г. «Об утверждении Доктрины информационной безопасности Российской Федерации»
13. Приказ Президента Российской Федерации № Пр-1753 от 24 июля 2013 г. «Об утверждении Основ государственной политики в области международной информационной безопасности на период до 2020 года»
14. Распоряжение Правительства Российской Федерации № 2036-р от 01 ноября 2013 года «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года» // Собрание законодательства Российской Федерации. - 2013. №46. - Ст. 5954
15. Распоряжение Совета Безопасности Российской Федерации от 07 марта 2008 года «Об утверждении Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации»
16. Выписка из Концепция № К 1274 от 12 декабря 2014 г. «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
17. Выписка из Концепции от 22 сентября 2011 г. «Конвенция об обеспечении международной информационной безопасности»
18. Проект Концепции Совета Федерации Российской Федерации от 28 ноября 2013 г. «Концепция Стратегии кибербезопасности Российской Федерации»
19. Проект Концепции Совета Безопасности Российской Федерации от 09 сентября 1999 года «Концепция совершенствования правового обеспечения информационной безопасности Российской Федерации»
20. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) № 31 от 14 марта 2014 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
21. Приказ Федерального агентства по техническому регулированию и метрологии №1493-Ст от 10 ноября 2014 г. «Об утверждении Национального стандарта Российской Федерации № ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Сети коммуникационные промышленные: защищённость (кибербезопасность) сети и системы»
22. «Окинавская хартия Глобального информационного общества» от 21 июля 2000 г. <http://kremlin.ru/supplement/3170> (дата обращения: 30.04.2017)
23. «Тунисское обязательство» № WSIS-05/TUNIS/DOC/7-R от 15 ноября 2005 г. // Всемирная встреча на высшем уровне по вопросам информационного общества, Тунис.
24. Декларация принципов № WSIS-03/GENEVA/DOC/4-R от 12 декабря 2003 г. «Построение информационного общества - глобальная задача в новом тысячелетии» // Всемирная встреча на высшем уровне по вопросам информационного общества, Женева.
25. «План действий» № WSIS-03/GENEVA/DOC/5-R от 12 декабря 2003 г. // Всемирная встреча на высшем уровне по вопросам информационного общества, Женева.
26. Программа Международного союза электросвязи от 16 апреля 2008 г. «Глобальная программа кибербезопасности: Основа для международного сотрудничества в области кибербезопасности»
27. Доклад Генеральной Ассамблеи Организации Объединённых Наций № A/55/140 от 10 июля 2000 г. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»
28. Доклад Генеральной Ассамблеи Организации Объединённых Наций № A/70/162 от 7 ноября 2015 г. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»
29. Резолюция Генеральной Ассамблеи Организации Объединённых Наций № A/RES/57/239 от 31 января 2003 г. «Создание глобальной культуры кибербезопасности»
30. Резолюция Генеральной Ассамблеи Организации Объединённых Наций № A/RES/55/63 от 22 января 2001 г. «Борьба с преступным использованием информационных технологий»
31. Резолюция Генеральной Ассамблеи Организации Объединённых Наций № A/RES/56/121 от 23 января 2002 г. «Борьба с преступным использованием информационных технологий»
32. Итоговый документ Международной Конференции от 19 мая 2005 года «ЮНЕСКО между двумя этапами Всемирного саммита по информационному обществу»
33. Доклад Всемирной организации интеллектуальной собственности от 15 августа 2016 года «Глобальный инновационный индекс»
34. The US Department of Defense Cyber Strategy от 17 апреля 2015 года
35. US National Security Strategy от 12 февраля 2015 года
36. «中华人民共和国国家安全法(2015年7月1日第十二届全国人民代表大会常务委员会第十五次会议通过中华人民共和国主席令第二十九号公布) //北大法宝引证码为» - Указ Председателя Китайской Народной Республики №29 от 1 июля 2015 г. «О вступлении в силу Закона Китайской Народной Республики «О национальной безопасности», принятого на 15-ой сессии Всекитайского собрания народных представителей» // Собрание законодательства КНР
37. EU Cyber Security Strategy – An Open, Safe and Secure Cyberspace от 07 февраля 2013 г.

**Литература**

**Монографии:**

1. Касенова М.Б., Демидов О.В. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Касенова М.Б., Демидов О.В. - М.: Статут, 2013. - 464 с.
2. Рогозин Д. Война и мир в терминах и определениях / Рогозин Д. - М.: Вече, 2016. - 272 с.

**Статьи:**

1. Боракий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) / Боракий Ю.В., Добродеев А.Ю., Бутусов И.В. // Вопросы кибербезопасности. - 2013. №1. - С.2-9
2. Боракий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) / Боракий Ю.В., Добродеев А.Ю., Бутусов И.В. // Вопросы кибербезопасности. - 2014. №1. - С.5-12
3. Безкоровайный М.М. Кибербезопасность - подходы к определению понятия / Безкоровайный М.М., Татузов А.Л. // Вопросы кибербезопасности. - 2014. №4. - С.22 - 27
4. Зубарев И.В. Кибербезопасность автоматизированных систем управления военного назначения / Зубарев И.В., Жидков И.В., Кадушкин И.В. // Вопросы кибербезопасности. - 2013. №1. - С.10-16
5. Згоба А.И. Кибербезопасность: угрозы, вызовы, решения / Згоба А.И., Маркелов Д.В., Смирнов П.И. // Вопросы кибербезопасности. - 2014. №5. - С.30-38
6. Марков А.С. Руководящие указания по кибербезопасности в контексте ISO 27032 / Марков А.С., Цирлов В.Л. // Вопросы кибербезопасности. - 2014. №1. - С.28-35
7. Карпова Д.Н. Киберпреступность: глобальная проблема и её решение / Карпова Д.Н. // Власть. - 2014. №8. - С.46-50
8. Шушков Г.М. Концептуальные основы информационной безопасности Российской Федерации / Шушков Г.М., Сергеев И.В. // Актуальные вопросы научной и научно-педагогической деятельности молодых учёных: сборник научных трудов III Всероссийской заочной научно-практической конференции. - М.: ИИУ МГОУ, 2016. - С.69-76
9. Воронцов С.А. Политическая культура и идеологии: О необходимости совершенствования подходов к обеспечению национальной безопасности России в информационной сфере / Воронцов С.А., Штейнбух А.Г. // Наука и образование: хозяйство и экономика; предпринимательство; право и управлние. - 2015. №9. - С.16-25
10. Федоров А. Проблемы информационной безопасности сегодня: Алогизмы развития / Федоров А. // Индекс безопасности. - М.: Пир-Центр, 2012. №1. - С. 261-270
11. Самохина Н.Н. Феномен идеологии экстремизма и терроризма в сети интернет: Проблемы и пути их решения / Самохина Н.Н., Готова С.Г. // Общество: политика, экономика, право. - 2016. №10. - С. 18-23
12. Троегубов Ю.Н. Проблемы противодействия экстремизму в сети интернет / Троегубов Ю.Н. // Гуманитарный вектор. Серия: История, политология. - 2014. №3. - С.143-147
13. Майдыков А.А. Национальные интересы - Актуальные проблемы противодействия использованию интернета террористическими и экстремистским организациями / Майдыков А.А., Исаров О.Б. // Национальные интересы: приоритеты и безопасность. - 2015. №38. - С.44-51
14. Ельчанинова Н.Б. Проблемы правовой охраны интеллектуальной собственности в сети интернет / Ельчанинова Н.Б. // Общество: политика, экономика, право. - 2016. №12. - С. 11-15
15. Глазунов О.Н. Специфика правового регулирования сети интернет в Китайской Народной Республике / Глазунов О.Н., Авдеенко В.В. // Общество: политика, экономика, право. - 2017. №2. - С. 19-23
16. Казаковцев А.В. НАТО и кибербезопасность / Казаковцев А.В. // Вестник Волгоградского государственного университета. - 2012. №2. - С.109-114
17. Бухарин В.В. Сравнительный анализ нормативной базы по обеспечению информационной безопасности в США и РФ (конец XX - начало XXI века) / Бухарин В.В. // Вестник Иркутского государственного технического университета. - 2016. №20. - С.101-108
18. Морозов И.Л. Информационная безопасность политической системы / Морозов И.Л. // Полис. Политические исследования. - 2002. №5. - С.134-145
19. Karaman M., Catalkaya H., Aybar C. Institutional Cybersecurity from Military Perspective / Karaman M., Catalkaya H., Aybar C. // International Journal of Information Security Science. - 2016. №1. - P.1-7.
20. Gozzi R. A brief history of internet time / Gozzi R. // Metaphors in action - 2002. №1 - P.47-54
21. Rohrig W. Cyber Security and Cyber Defense in the European Union / Rohig W. // Cyber Security Review - 2014. №2 - P.7-16
22. Gharibi W., Adamov A., Hahanov V. Security Risks and Modern Cyber Security Technologies for Corporate Networks / Gharibi W., Adamov A., Hahanov // Radiotech and information - 2010. №4 - P.31-35

**Справочно-энциклопедическая литература:**

1. Российский статистический ежегодник 2014: «Ежегодный мониторинг средств, выделяемых из федерального бюджета на финансирование НИОКР» / Аналитический центр при Правительстве Российской Федерации, 2014 - 31 с.
2. Российский статистический ежегодник 2016: «Финансы России» / Федеральная служба государственной статистики. Росстат, 2016. Ред. Егоренко С.Н. - М., 2016. - 343 с.
3. Российский статистический ежегодник 2016: «Россия в цифрах» / Федеральная служба государственной статистики. Росстат, 2016. Ред. Суринов А.Е. - М., 2016. - 543 с.
4. Gross domestic product ranking от 17 апреля 2017 года / Всемирный банк. – 2017. – 4 с.

**Официальные сайты организаций:**

1. NATO Cooperative Cyber Defense Centre of Excellence, Definition Centre <https://ccdcoe.org/cyber-definitions.html> (Дата обращения: 25.04.2017)
2. UNESCO Institute for Statistics <http://uis.unesco.org/> (Дата обращения: 27.04.2017)
3. Internet World Stats <http://www.internetworldstats.com/stats.htm> (Дата обращения: 27.04.2017)
4. Журнал документов Организации Объединённых Наций <https://search.un.org/index.php?lang=ru> (Дата обращения: 20.04.2017)

**Материалы сети интернет:**

1. Барри Ч. Взгляд на национальные и международные проблемы кибербезопасности / Барри Ч. - 2015. - URL: <https://digital.report/charlz-barri-o-podhodah-ssha-i-nato-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasnosti/> (Дата обращения: 23.04.2017)
2. РиаНовости: Громкие случаи кибератак и взломов в мире в 2000-2014 годах / РиаНовости - 2014.- URL: <https://ria.ru/spravka/20140814/1019983404.html> (Дата обращения: 27.04.2017)
3. SecurityLab: Пентагон намерен расширить сотрудничество с частным секторов в борьбе к киберпреступностью / SecurityLab - 2012. - URL: <http://www.securitylab.ru/news/424454.php> (Дата обращения: 27.04.2017)
4. BBC: Во взломе сервера Демократической партии США сознался хакер-одиночки / BBC - 2016. - URL: <http://www.bbc.com/russian/news/2016/06/160616_hackers_usa_democratic_party> (Дата обращения: 27.04.2017)
5. Русское Агентство Новостей: Вирус WannaCry атаковал Минздрав, МЧС, МВД, РЖД, «Сбербанк» и «Мегафон» / Русское Агентство Новостей - 2017. - URL: [новости-россии.ru-an.info/новости/вирус-wanna-cry-атаковал-минздрав-мчс-мвд-ржд-сбербанк-и-мегафон/](http://xn----ctbsbazhbctieai.ru-an.info/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/%D0%B2%D0%B8%D1%80%D1%83%D1%81-wanna-cry-%D0%B0%D1%82%D0%B0%D0%BA%D0%BE%D0%B2%D0%B0%D0%BB-%D0%BC%D0%B8%D0%BD%D0%B7%D0%B4%D1%80%D0%B0%D0%B2-%D0%BC%D1%87%D1%81-%D0%BC%D0%B2%D0%B4-%D1%80%D0%B6%D0%B4-%D1%81%D0%B1%D0%B5%D1%80%D0%B1%D0%B0%D0%BD%D0%BA-%D0%B8-%D0%BC%D0%B5%D0%B3%D0%B0%D1%84%D0%BE%D0%BD/) (Дата обращения: 14.05.2017)
6. Wylsa: Что известно про вирус  WannaCry и как не попасть? / Wylsa - 2017. - URL: <https://wylsa.com/wannacry-virus/> (Дата обращения: 14.05.2017)
7. ТАСС: Крупные атаки хакеров в 2001-2016 годах: хронология / ТАСС – 2016. - URL: <http://tass.ru/info/1408961> (Дата обращения: 22.04.2017)
8. ГазетаРу: Порошенко готовится к кибервойне / ГазетаРу – 2017. – URL: <https://www.gazeta.ru/politics/2017/05/16_a_10675793.shtml> (Дата обращения: 16.05.2017)
9. Коммерсант: Концепция кибербезопасности разошлась с государственной стратегией / Коммерсант – 2013. – URL: <https://www.kommersant.ru/doc/2355154> (Дата обращения: 21.04.2017)
10. BBC: «Российский след» на выборах президента США: так были ли хакеры? / BBC – 2016. – URL: <http://www.bbc.com/russian/features-38205035> (Дата обращения: 23.04.2017)
11. BBC: Макрон: наши серверы взломаны хакерами / BBC – 2017. – URL: <http://www.bbc.com/russian/news-39829217> (Дата обращения: 06.05.2017)

1. Проект Концепции Совета Федерации Российской Федерации от 28 ноября 2013 г. «Концепция Стратегии кибербезопасности Российской Федерации» [↑](#footnote-ref-2)
2. Коммерсант: Концепция кибербезопасности разошлась с государственной стратегией / Коммерсант – 2013. – URL: <https://www.kommersant.ru/doc/2355154> (Дата обращения: 21.04.2017) [↑](#footnote-ref-3)
3. Gozzi R. A brief history of internet time / Gozzi R. // Metaphors in action - 2002. №1 - P.47-54 [↑](#footnote-ref-4)
4. Боракий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) / Боракий Ю.В., Добродеев А.Ю., Бутусов И.В. // Вопросы кибербезопасности. - 2013. №1. - С.2-9 [↑](#footnote-ref-5)
5. Рогозин Д. Война и мир в терминах и определениях / Рогозин Д. - М.: Вече, 2016. - 272 с. [↑](#footnote-ref-6)
6. Федоров А. Проблемы информационной безопасности сегодня: Алогизмы развития / Федоров А. // Индекс безопасности. - М.: Пир-Центр, 2012. №1. - С. 261-270 [↑](#footnote-ref-7)
7. РиаНовости: Громкие случаи кибератак и взломов в мире в 2000-2014 годах / РиаНовости - 2014.- URL: https://ria.ru/spravka/20140814/1019983404.html (Дата обращения: 27.04.2017) [↑](#footnote-ref-8)
8. Воронцов С.А. Политическая культура и идеологии: О необходимости совершенствования подходов к обеспечению национальной безопасности России в информационной сфере / Воронцов С.А., Штейнбух А.Г. // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. - 2015. №9. - С.16-25 [↑](#footnote-ref-9)
9. Самохина Н.Н. Феномен идеологии экстремизма и терроризма в сети интернет: Проблемы и пути их решения / Самохина Н.Н., Готова С.Г. // Общество: политика, экономика, право. - 2016. №10. - С. 18-23 [↑](#footnote-ref-10)
10. Воронцов С.А. Политическая культура и идеологии: О необходимости совершенствования подходов к обеспечению национальной безопасности России в информационной сфере / Воронцов С.А., Штейнбух А.Г. // Наука и образование: хозяйство и экономика; предпринимательство; право и управлние. - 2015. №9. - С.16-25 [↑](#footnote-ref-11)
11. ТАСС: Крупные атаки хакеров в 2001-2016 годах: хронология / ТАСС – 2016. - URL: <http://tass.ru/info/1408961> (Дата обращения: 22.04.2017) [↑](#footnote-ref-12)
12. BBC: «Российский след» на выборах президента США: так были ли хакеры? / BBC – 2016. – URL: <http://www.bbc.com/russian/features-38205035> (Дата обращения: 23.04.2017) [↑](#footnote-ref-13)
13. BBC: Макрон: наши серверы взломаны хакерами / BBC – 2017. – URL: <http://www.bbc.com/russian/news-39829217> (Дата обращения: 06.05.2017) [↑](#footnote-ref-14)
14. Шушков Г.М. Концептуальные основы информационной безопасности Российской Федерации / Шушков Г.М., Сергеев И.В. // Актуальные вопросы научной и научно-педагогической деятельности молодых учёных: сборник научных трудов III Всероссийской заочной научно-практической конференции. - М.: ИИУ МГОУ, 2016. - С.69-76 [↑](#footnote-ref-15)
15. Gozzi R. A brief history of internet time / Gozzi R. // Metaphors in action - 2002. №1 - P.47-54 [↑](#footnote-ref-16)
16. Казаковцев А.В. НАТО и кибербезопасность / Казаковцев А.В. // Вестник Волгоградского государственного университета. - 2012. №2. - С.109-114 [↑](#footnote-ref-17)
17. Касенова М.Б., Демидов О.В. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Касенова М.Б., Демидов О.В. - М.: Статут, 2013. - 464 с. [↑](#footnote-ref-18)
18. Боракий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) / Боракий Ю.В., Добродеев А.Ю., Бутусов И.В. // Вопросы кибербезопасности. - 2014. №1. - С.5-12 [↑](#footnote-ref-19)
19. Боракий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) / Боракий Ю.В., Добродеев А.Ю., Бутусов И.В. // Вопросы кибербезопасности. - 2013. №1. - С.2-9 [↑](#footnote-ref-20)
20. Безкоровайный М.М. Кибербезопасность - подходы к определению понятия / Безкоровайный М.М., Татузов А.Л. // Вопросы кибербезопасности. - 2014. №4. - С.22 - 27 [↑](#footnote-ref-21)
21. Казаковцев А.В. НАТО и кибербезопасность / Казаковцев А.В. // Вестник Волгоградского государственного университета. - 2012. №2. - С.109-114 [↑](#footnote-ref-22)
22. Gozzi R. A brief history of internet time / Gozzi R. // Metaphors in action - 2002. №1 - P.47-54 [↑](#footnote-ref-23)
23. Karaman M., Catalkaya H., Aybar C. Institutional Cybersecurity from Military Perspective / Karaman M., Catalkaya H., Aybar C. // International Journal of Information Security Science. - 2016. №1. - P.1-7. [↑](#footnote-ref-24)
24. Касенова М.Б., Демидов О.В. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Касенова М.Б., Демидов О.В. - М.: Статут, 2013. - 464 с. [↑](#footnote-ref-25)
25. Марков А.С. Руководящие указания по кибербезопасности в контексте ISO 27032 / Марков А.С., Цирлов В.Л. // Вопросы кибербезопасности. - 2014. №1. - С.28-35 [↑](#footnote-ref-26)
26. Згоба А.И. Кибербезопасность: угрозы, вызовы, решения / Згоба А.И., Маркелов Д.В., Смирнов П.И. // Вопросы кибербезопасности. - 2014. №5. - С.30-38 [↑](#footnote-ref-27)
27. Бухарин В.В. Сравнительный анализ нормативной базы по обеспечению информационной безопасности в США и РФ (конец XX - начало XXI века) / Бухарин В.В. // Вестник Иркутского государственного технического университета. - 2016. №20. - С.101-108 [↑](#footnote-ref-28)
28. The US Department of Defense Cyber Strategy от 17 апреля 2015 года [↑](#footnote-ref-29)
29. Karaman M., Catalkaya H., Aybar C. Institutional Cybersecurity from Military Perspective / Karaman M., Catalkaya H., Aybar C. // International Journal of Information Security Science. - 2016. №1. - P.1-7. [↑](#footnote-ref-30)
30. Rohrig W. Cyber Security and Cyber Defense in the European Union / Rohig W. // Cyber Security Review - 2014. №2 - P.7-16 [↑](#footnote-ref-31)
31. РиаНовости: Громкие случаи кибератак и взломов в мире в 2000-2014 годах / РиаНовости - 2014.- URL: <https://ria.ru/spravka/20140814/1019983404.html> (Дата обращения: 27.04.2017) [↑](#footnote-ref-32)
32. NATO Cooperative Cyber Defense Centre of Excellence, Definition Centre <https://ccdcoe.org/cyber-definitions.html> (Дата обращения: 25.04.2017) [↑](#footnote-ref-33)
33. Бухарин В.В. Сравнительный анализ нормативной базы по обеспечению информационной безопасности в США и РФ (конец XX - начало XXI века) / Бухарин В.В. // Вестник Иркутского государственного технического университета. - 2016. №20. - С.101-108 [↑](#footnote-ref-34)
34. Казаковцев А.В. НАТО и кибербезопасность / Казаковцев А.В. // Вестник Волгоградского государственного университета. - 2012. №2. - С.109-114 [↑](#footnote-ref-35)
35. NATO Cooperative Cyber Defense Centre of Excellence, Definition Centre <https://ccdcoe.org/cyber-definitions.html> (Дата обращения: 25.04.2017) [↑](#footnote-ref-36)
36. Приказ Президента Российской Федерации № Пр-212 от 07 сентября 2000 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» [↑](#footnote-ref-37)
37. Проект Концепции Совета Безопасности Российской Федерации от 09 сентября 1999 года «Концепция совершенствования правового обеспечения информационной безопасности Российской Федерации» [↑](#footnote-ref-38)
38. Выписка из Концепции от 22 сентября 2011 г. «Конвенция об обеспечении международной информационной безопасности» [↑](#footnote-ref-39)
39. Приказ Президента Российской Федерации № Пр-1753 от 24 июля 2013 г. «Об утверждении Основ государственной политики в области международной информационной безопасности на период до 2020 года» [↑](#footnote-ref-40)
40. Распоряжение Совета Безопасности Российской Федерации от 07 марта 2008 года «Об утверждении Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации» [↑](#footnote-ref-41)
41. Приказ Президента Российской Федерации № Пр-212 от 07 сентября 2000 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» [↑](#footnote-ref-42)
42. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074 [↑](#footnote-ref-43)
43. Бухарин В.В. Сравнительный анализ нормативной базы по обеспечению информационной безопасности в США и РФ (конец XX - начало XXI века) / Бухарин В.В. // Вестник Иркутского государственного технического университета. - 2016. №20. - С.101-108 [↑](#footnote-ref-44)
44. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074 [↑](#footnote-ref-45)
45. The US Department of Defense Cyber Strategy от 17 апреля 2015 года [↑](#footnote-ref-46)
46. Казаковцев А.В. НАТО и кибербезопасность / Казаковцев А.В. // Вестник Волгоградского государственного университета. - 2012. №2. - С.109-114 [↑](#footnote-ref-47)
47. Барри Ч. Взгляд на национальные и международные проблемы кибербезопасности / Барри Ч. - 2015. - URL: <https://digital.report/charlz-barri-o-podhodah-ssha-i-nato-v-oblasti-mezhdunarodnoy-informatsionnoy-bezopasnosti/> (Дата обращения: 23.04.2017) [↑](#footnote-ref-48)
48. Ельчанинова Н.Б. Проблемы правовой охраны интеллектуальной собственности в сети интернет / Ельчанинова Н.Б. // Общество: политика, экономика, право. - 2016. №12. - С. 11-15 [↑](#footnote-ref-49)
49. Казаковцев А.В. НАТО и кибербезопасность / Казаковцев А.В. // Вестник Волгоградского государственного университета. - 2012. №2. - С.109-114 [↑](#footnote-ref-50)
50. SecurityLab: Пентагон намерен расширить сотрудничество с частным секторов в борьбе к киберпреступностью / SecurityLab - 2012. - URL: <http://www.securitylab.ru/news/424454.php> (Дата обращения: 27.04.2017) [↑](#footnote-ref-51)
51. РиаНовости: Громкие случаи кибератак и взломов в мире в 2000-2014 годах / РиаНовости - 2014.- URL: <https://ria.ru/spravka/20140814/1019983404.html> (Дата обращения: 27.04.2017) [↑](#footnote-ref-52)
52. BBC: Во взломе сервера Демократической партии США сознался хакер-одиночки / BBC - 2016. - URL: <http://www.bbc.com/russian/news/2016/06/160616_hackers_usa_democratic_party> (Дата обращения: 27.04.2017) [↑](#footnote-ref-53)
53. Самохина Н.Н. Феномен идеологии экстремизма и терроризма в сети интернет: Проблемы и пути их решения / Самохина Н.Н., Готова С.Г. // Общество: политика, экономика, право. - 2016. №10. - С. 18-23 [↑](#footnote-ref-54)
54. ТАСС: Крупные атаки хакеров в 2001-2016 годах: хронология / ТАСС – 2016. - URL: <http://tass.ru/info/1408961> [↑](#footnote-ref-55)
55. Карпова Д.Н. Киберпреступность: глобальная проблема и её решение / Карпова Д.Н. // Власть. - 2014. №8. - С.46-50 [↑](#footnote-ref-56)
56. Троегубов Ю.Н. Проблемы противодействия экстремизму в сети интернет / Троегубов Ю.Н. // Гуманитарный вектор. Серия: История, политология. - 2014. №3. - С.143-147 [↑](#footnote-ref-57)
57. РиаНовости: Громкие случаи кибератак и взломов в мире в 2000-2014 годах / РиаНовости - 2014.- URL: <https://ria.ru/spravka/20140814/1019983404.html> (Дата обращения: 27.04.2017) [↑](#footnote-ref-58)
58. Майдыков А.А. Национальные интересы - Актуальные проблемы противодействия использованию интернета террористическими и экстремистским организациями / Майдыков А.А., Исаров О.Б. // Национальные интересы: приоритеты и безопасность. - 2015. №38. - С.44-51 [↑](#footnote-ref-59)
59. Воронцов С.А. Политическая культура и идеологии: О необходимости совершенствования подходов к обеспечению национальной безопасности России в информационной сфере / Воронцов С.А., Штейнбух А.Г. // Наука и образование: хозяйство и экономика; предпринимательство; право и управлние. - 2015. №9. - С.16-25 [↑](#footnote-ref-60)
60. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074 [↑](#footnote-ref-61)
61. Згоба А.И. Кибербезопасность: угрозы, вызовы, решения / Згоба А.И., Маркелов Д.В., Смирнов П.И. // Вопросы кибербезопасности. - 2014. №5. - С.30-38 [↑](#footnote-ref-62)
62. US National Security Strategy от 12 февраля 2015 года [↑](#footnote-ref-63)
63. The US Department of Defense Cyber Strategy от 17 апреля 2015 года [↑](#footnote-ref-64)
64. Боракий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) / Боракий Ю.В., Добродеев А.Ю., Бутусов И.В. // Вопросы кибербезопасности. - 2014. №1. - С.5-12 [↑](#footnote-ref-65)
65. Безкоровайный М.М. Кибербезопасность - подходы к определению понятия / Безкоровайный М.М., Татузов А.Л. // Вопросы кибербезопасности. - 2014. №4. - С.22 - 27 [↑](#footnote-ref-66)
66. Русское Агентство Новостей: Вирус WannaCry атаковал Минздрав, МЧС, МВД, РЖД, «Сбербанк» и «Мегафон» / Русское Агентство Новостей - 2017. - URL: [новости-россии.ru-an.info/новости/вирус-wanna-cry-атаковал-минздрав-мчс-мвд-ржд-сбербанк-и-мегафон/](http://xn----ctbsbazhbctieai.ru-an.info/%D0%BD%D0%BE%D0%B2%D0%BE%D1%81%D1%82%D0%B8/%D0%B2%D0%B8%D1%80%D1%83%D1%81-wanna-cry-%D0%B0%D1%82%D0%B0%D0%BA%D0%BE%D0%B2%D0%B0%D0%BB-%D0%BC%D0%B8%D0%BD%D0%B7%D0%B4%D1%80%D0%B0%D0%B2-%D0%BC%D1%87%D1%81-%D0%BC%D0%B2%D0%B4-%D1%80%D0%B6%D0%B4-%D1%81%D0%B1%D0%B5%D1%80%D0%B1%D0%B0%D0%BD%D0%BA-%D0%B8-%D0%BC%D0%B5%D0%B3%D0%B0%D1%84%D0%BE%D0%BD/) (Дата обращения: 14.05.2017) [↑](#footnote-ref-67)
67. Касенова М.Б., Демидов О.В. Кибербезопасность и управление интернетом: Документы и материалы для российских регуляторов и экспертов / Касенова М.Б., Демидов О.В. - М.: Статут, 2013. - 464 с. [↑](#footnote-ref-68)
68. Боракий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) / Боракий Ю.В., Добродеев А.Ю., Бутусов И.В. // Вопросы кибербезопасности. - 2013. №1. - С.2-9 [↑](#footnote-ref-69)
69. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074 [↑](#footnote-ref-70)
70. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074 [↑](#footnote-ref-71)
71. Приказ Президента Российской Федерации № Пр-1753 от 24 июля 2013 г. «Об утверждении Основ государственной политики в области международной информационной безопасности на период до 2020 года» [↑](#footnote-ref-72)
72. Доклад Генеральной Ассамблеи Организации Объединённых Наций № A/70/162 от 7 ноября 2015 г. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» [↑](#footnote-ref-73)
73. Боракий Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) / Боракий Ю.В., Добродеев А.Ю., Бутусов И.В. // Вопросы кибербезопасности. - 2014. №1. - С.5-12 [↑](#footnote-ref-74)
74. The US Department of Defense Cyber Strategy от 17 апреля 2015 года [↑](#footnote-ref-75)
75. US National Security Strategy от 12 февраля 2015 года [↑](#footnote-ref-76)
76. Морозов И.Л. Информационная безопасность политической системы / Морозов И.Л. // Полис. Политические исследования. - 2002. №5. - С.134-145 [↑](#footnote-ref-77)
77. Internet World Stats <http://www.internetworldstats.com/stats.htm> (Дата обращения: 27.04.2017) [↑](#footnote-ref-78)
78. Глазунов О.Н. Специфика правового регулирования сети интернет в Китайской Народной Республике / Глазунов О.Н., Авдеенко В.В. // Общество: политика, экономика, право. - 2017. №2. - С. 19-23 [↑](#footnote-ref-79)
79. «中华人民共和国国家安全法(2015年7月1日第十二届全国人民代表大会常务委员会第十五次会议通过中华人民共和国主席令第二十九号公布) //北大法宝引证码为» - Указ Председателя Китайской Народной Республики №29 от 1 июля 2015 г. «О вступлении в силу Закона Китайской Народной Республики «О национальной безопасности», принятого на 15-ой сессии Всекитайского собрания народных представителей» // Собрание законодательства КНР [↑](#footnote-ref-80)
80. Глазунов О.Н. Специфика правового регулирования сети интернет в Китайской Народной Республике / Глазунов О.Н., Авдеенко В.В. // Общество: политика, экономика, право. - 2017. №2. - С. 19-23 [↑](#footnote-ref-81)
81. Безкоровайный М.М. Кибербезопасность - подходы к определению понятия / Безкоровайный М.М., Татузов А.Л. // Вопросы кибербезопасности. - 2014. №4. - С.22 - 27 [↑](#footnote-ref-82)
82. Выписка из Концепция № К 1274 от 12 декабря 2014 г. «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [↑](#footnote-ref-83)
83. Указ Президента Российской Федерации № 203 от 9 мая 2017 г. «О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [↑](#footnote-ref-84)
84. Казаковцев А.В. НАТО и кибербезопасность / Казаковцев А.В. // Вестник Волгоградского государственного университета. - 2012. №2. - С.109-114 [↑](#footnote-ref-85)
85. Шушков Г.М. Концептуальные основы информационной безопасности Российской Федерации / Шушков Г.М., Сергеев И.В. // Актуальные вопросы научной и научно-педагогической деятельности молодых учёных: сборник научных трудов III Всероссийской заочной научно-практической конференции. - М.: ИИУ МГОУ, 2016. - С.69-76 [↑](#footnote-ref-86)
86. Программа Международного союза электросвязи от 16 апреля 2008 г. «Глобальная программа кибербезопасности: Основа для международного сотрудничества в области кибербезопасности» [↑](#footnote-ref-87)
87. Шушков Г.М. Концептуальные основы информационной безопасности Российской Федерации / Шушков Г.М., Сергеев И.В. // Актуальные вопросы научной и научно-педагогической деятельности молодых учёных: сборник научных трудов III Всероссийской заочной научно-практической конференции. - М.: ИИУ МГОУ, 2016. - С.69-76 [↑](#footnote-ref-88)
88. Приказ Президента Российской Федерации № Пр-212 от 07 сентября 2000 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» [↑](#footnote-ref-89)
89. Закон Российской Федерации №5485-1 от 21 июля 1993 г. «О государственной тайне» // Собрание законодательства Российской Федерации. - 1997. №41. [↑](#footnote-ref-90)
90. Указ Президента Российской Федерации № 1286 от 06 октября 2004 г. «Вопросы Межведомственной комиссии по защите государственной тайны» // Собрание законодательства Российской Федерации. - 2004. №41. - Ст. 4024 [↑](#footnote-ref-91)
91. Выписка из Концепция № К 1274 от 12 декабря 2014 г. «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [↑](#footnote-ref-92)
92. Конституция Российской Федерации от 12 декабря 1993 г. // Собрание законодательства Российской Федерации. - 2014. №31. - Ст. 4398 [↑](#footnote-ref-93)
93. Кодекс Российской Федерации № 63-ФЗ от 13 июня 1996 г. «Уголовный кодекс Российской Федерации» [↑](#footnote-ref-94)
94. Кодекс Российской Федерации № 195-ФЗ от 30 декабря 2001 г. «Об административных правонарушениях» // Собрание законодательства Российской Федерации. - 2002. №1. - Ст. 1 [↑](#footnote-ref-95)
95. Указ Президента Российской Федерации № 203 от 9 мая 2017 г. «О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [↑](#footnote-ref-96)
96. Указ Президента Российской Федерации № 803 от 03 февраля 2012 г. «Об утверждении Основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» [↑](#footnote-ref-97)
97. Распоряжение Совета Безопасности Российской Федерации от 07 марта 2008 года «Об утверждении Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации» [↑](#footnote-ref-98)
98. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) № 31 от 14 марта 2014 г. «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [↑](#footnote-ref-99)
99. Указ Президента Российской Федерации № 683 от 31 декабря 2015 г. «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №1. - Ст. 212 [↑](#footnote-ref-100)
100. Зубарев И.В. Кибербезопасность автоматизированных систем управления военного назначения / Зубарев И.В., Жидков И.В., Кадушкин И.В. // Вопросы кибербезопасности. - 2013. №1. - С.10-16 [↑](#footnote-ref-101)
101. SecurityLab: Пентагон намерен расширить сотрудничество с частным секторов в борьбе к киберпреступностью / SecurityLab - 2012. - URL: <http://www.securitylab.ru/news/424454.php> (Дата обращения: 27.04.2017) [↑](#footnote-ref-102)
102. Rohrig W. Cyber Security and Cyber Defense in the European Union / Rohig W. // Cyber Security Review - 2014. №2 - P.7-16 [↑](#footnote-ref-103)
103. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074 [↑](#footnote-ref-104)
104. Российский статистический ежегодник 2016: «Финансы России» / Федеральная служба государственной статистики. Росстат, 2016. Ред. Егоренко С.Н. - М., 2016. - 343 с. [↑](#footnote-ref-105)
105. Российский статистический ежегодник 2014: «Ежегодный мониторинг средств, выделяемых из федерального бюджета на финансирование НИОКР» / Аналитический центр при Правительстве Российской Федерации, 2014 - 31 с. [↑](#footnote-ref-106)
106. UNESCO Institute for Statistics <http://uis.unesco.org/> (Дата обращения: 27.04.2017) [↑](#footnote-ref-107)
107. Доклад Генеральной Ассамблеи Организации Объединённых Наций № A/70/162 от 7 ноября 2015 г. «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности» [↑](#footnote-ref-108)
108. Казаковцев А.В. НАТО и кибербезопасность / Казаковцев А.В. // Вестник Волгоградского государственного университета. - 2012. №2. - С.109-114 [↑](#footnote-ref-109)
109. The US Department of Defense Cyber Strategy от 17 апреля 2015 года [↑](#footnote-ref-110)
110. Шушков Г.М. Концептуальные основы информационной безопасности Российской Федерации / Шушков Г.М., Сергеев И.В. // Актуальные вопросы научной и научно-педагогической деятельности молодых учёных: сборник научных трудов III Всероссийской заочной научно-практической конференции. - М.: ИИУ МГОУ, 2016. - С.69-76 [↑](#footnote-ref-111)
111. Rohrig W. Cyber Security and Cyber Defense in the European Union / Rohig W. // Cyber Security Review - 2014. №2 - P.7-16 [↑](#footnote-ref-112)
112. Указ Президента Российской Федерации № 203 от 9 мая 2017 г. «О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [↑](#footnote-ref-113)
113. Российский статистический ежегодник 2016: «Россия в цифрах» / Федеральная служба государственной статистики. Росстат, 2016. Ред. Суринов А.Е. - М., 2016. - 543 с. [↑](#footnote-ref-114)
114. Gharibi W., Adamov A., Hahanov V. Security Risks and Modern Cyber Security Technologies for Corporate Networks / Gharibi W., Adamov A., Hahanov // Radiotech and information - 2010. №4 - P.31-35 [↑](#footnote-ref-115)
115. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074 [↑](#footnote-ref-116)
116. Указ Президента Российской Федерации № 203 от 9 мая 2017 г. «О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [↑](#footnote-ref-117)
117. Морозов И.Л. Информационная безопасность политической системы / Морозов И.Л. // Полис. Политические исследования. - 2002. №5. - С.134-145 [↑](#footnote-ref-118)
118. Карпова Д.Н. Киберпреступность: глобальная проблема и её решение / Карпова Д.Н. // Власть. - 2014. №8. - С.46-50 [↑](#footnote-ref-119)
119. Казаковцев А.В. НАТО и кибербезопасность / Казаковцев А.В. // Вестник Волгоградского государственного университета. - 2012. №2. - С.109-114 [↑](#footnote-ref-120)
120. The US Department of Defense Cyber Strategy от 17 апреля 2015 года [↑](#footnote-ref-121)
121. «中华人民共和国国家安全法(2015年7月1日第十二届全国人民代表大会常务委员会第十五次会议通过中华人民共和国主席令第二十九号公布) //北大法宝引证码为» - Указ Председателя Китайской Народной Республики №29 от 1 июля 2015 г. «О вступлении в силу Закона Китайской Народной Республики «О национальной безопасности», принятого на 15-ой сессии Всекитайского собрания народных представителей» // Собрание законодательства КНР [↑](#footnote-ref-122)
122. EU Cyber Security Strategy – An Open, Safe and Secure Cyberspace от 07 февраля 2013 г. [↑](#footnote-ref-123)
123. Rohrig W. Cyber Security and Cyber Defense in the European Union / Rohig W. // Cyber Security Review - 2014. №2 - P.7-16 [↑](#footnote-ref-124)
124. Доклад Всемирной организации интеллектуальной собственности от 15 августа 2016 года «Глобальный инновационный индекс» [↑](#footnote-ref-125)
125. UNESCO Institute for Statistics <http://uis.unesco.org/> (Дата обращения: 27.04.2017) [↑](#footnote-ref-126)
126. Gross domestic product ranking от 17 апреля 2017 года / Всемирный банк. – 2017. – 4 с. [↑](#footnote-ref-127)
127. Wylsa: Что известно про вирус  WannaCry и как не попасть? / Wylsa - 2017. - URL: <https://wylsa.com/wannacry-virus/> (Дата обращения: 14.05.2017) [↑](#footnote-ref-128)
128. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074 [↑](#footnote-ref-129)
129. Указ Президента Российской Федерации № 203 от 9 мая 2017 г. «О стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [↑](#footnote-ref-130)
130. ГазетаРу: Порошенко готовится к кибервойне / ГазетаРу – 2017. – URL: <https://www.gazeta.ru/politics/2017/05/16_a_10675793.shtml> [↑](#footnote-ref-131)
131. Морозов И.Л. Информационная безопасность политической системы / Морозов И.Л. // Полис. Политические исследования. - 2002. №5. - С.134-145 [↑](#footnote-ref-132)
132. Федеральный закон №172-ФЗ от 28 июня 2014 г. «О стратегическом планировании в Российской Федерации» // Собрание законодательства Российской Федерации. - 2014. №26. - Ст. 3378 [↑](#footnote-ref-133)
133. Конституция Российской Федерации от 12 декабря 1993 г. // Собрание законодательства Российской Федерации. - 2014. №31. - Ст. 4398 [↑](#footnote-ref-134)
134. Указ Президента Российской Федерации № 683 от 31 декабря 2015 г. «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №1. - Ст. 212 [↑](#footnote-ref-135)
135. Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. - 2016. №50. - Ст. 7074 [↑](#footnote-ref-136)