Санкт-Петербургский государственный университет

***ТРИБУНЦЕВ Никита Александрович***

**Выпускная квалификационная работа**

***Киберопасности и киберугрозы в системе национальной безопасности современных государств***

Уровень образования: бакалавриат

Направление 41.03.04 "Политология"

Основная образовательная программа СВ.5027\* "Политология"

Научный руководитель:

профессор кафедры российской политики,
доктор политический наук,
Радиков Иван Владимирович

Рецензент:
доцент кафедры государственного и муниципального управления,

кандидат политических наук,
Ковалев Андрей Андреевич

Санкт-Петербург

2020

**ОГЛАВЛЕНИЕ**

[ВВЕДЕНИЕ 4](#_Toc41143244)

[Глава 1. КИБЕРБЕЗОПАСНОСТЬ КАК СОСТАВЛЯЮЩАЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ 11](#_Toc41143245)

[1.1 Основные подходы к понятиям «киберопасность» и «киберугроза» 11](#_Toc41143246)

[1.2 Диверсификация цифровой инфраструктуры как фактор современных киберугроз и киберопасностей 20](#_Toc41143247)

[1.3 Регулирование ответственного поведения государств в киберпространстве в контексте международной безопасности. 28](#_Toc41143248)

[Глава 2. КИБЕРОПАСНОСТИ И КИБЕРУГРОЗЫ В СТРАТЕГИЯХ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ГОСУДАРСТВ 34](#_Toc41143249)

[2.1 Стратегия национальной кибербезопасности США «Об основных киберугрозах» 34](#_Toc41143250)

[2.2 Государственные программы и стратегии КНР об угрозах и вызовах в сфере кибербезопасности. 40](#_Toc41143251)

[2.3 Государственные стратегии кибербезопасности государств Евросоюза об основных угрозах в киберпространстве. 47](#_Toc41143252)

[Глава 3. КИБЕРОПАСНОСТИ И КИБЕРУГРОЗЫ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА В СОВРЕМЕННОЙ РОССИИ 58](#_Toc41143253)

[3.1 Роль информационной безопасности в обеспечении суверенитета Российской Федерации 58](#_Toc41143254)

[3.2 Нормативные документы Российской Федерации по обеспечению информационной безопасности об опасностях и угрозах в киберпространстве. 64](#_Toc41143255)

[3.3 Перспективы защиты России от иностранных информационных интервенций и кибервоздействий. 68](#_Toc41143256)

[ЗАКЛЮЧЕНИЕ 75](#_Toc41143257)

[СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 78](#_Toc41143259)

**ВВЕДЕНИЕ**

Информационно-коммуникационные технологии, в течении последних 30 лет проникшие практически во все сферы жизни общества, стали причиной появления ряда явлений и процессов. Уровень развития IT - технологий, во многом определяет роль государства на международной арене. Глобальная информатизация общества является одной из доминирующих тенденций развития человеческой цивилизации в XXI в. Стремительному увеличение возможностей телекоммуникационных систем и новых информационных технологий приводит к формированию новой информационной среды обитания и жизнедеятельности людей.

Однако существует и обратная сторона данного явления. Очевидно, что вовлечение информационных технологий во все сферы жизнедеятельности, делает общество, зависимым от новейших технологий. Безопасность критической инфраструктуры, в настоящее время, напрямую зависит от надежности функционирования ее информационно-телекоммуникационной составляющей. Кроме того, совершенно ясно, что современные информационные технологии, ввиду ряда своих особенностей и преимуществ, могут быть использованы в преступных, террористических и военных целях. Таким образом, в настоящее время проблема обеспечения кибербезопасности на глобальном и национальном уровнях выдвинулась на центральное место в перечне вызовов национальной и международной безопасности.

**Актуальность** данной работы обусловлена:

- во-первых, кардинальными изменениями в области информационных технологий и смещением приоритетов в сторону киберпространства. Компьютерные технологии и сеть Интернет, активно используются для реализации общественных, экономических и политических целей.

-во-вторых, транснациональным характером киберпространства, при котором участники имеют возможность угрожать информационным системам различных стран из любой точки мира, как следствие, для борьбы с ними, необходимо высокоэффективное международное сотрудничество.

-в-третьих, расширением масштабов киберпреступности, кибертерроризма и киберэкстремизма, а также опасностью использования киберпространства в военных целях.

- в-четвертых, отсутствием в Российской Федерацией единой стратегии кибербезопасности.

**Степень научной разработанности.** При написании выпускной квалификационной работы автор опирался на теоретические работы и эмпирические исследования российских и зарубежных авторов по широкому спектру вопросов обеспечения политики информационной безопасности и кибербезопасности. Анализ литературы позволяет прийти к выводу, что вопросы последствий информатизации и обеспечения информационной безопасности хорошо изучены.

Прежде всего, стоит выделить работы Жаглина А.В[[1]](#footnote-1), Кершишнига Г[[2]](#footnote-2), Ирошникова Д.В[[3]](#footnote-3), Татузова А.Л. и Безкоровайного М.М[[4]](#footnote-4), в которых рассматриваются вопросы терминологии информационной безопасности и кибербезопасности.

Значительное внимание в данной исследовательской работе отведено проблеме международного сотрудничества в области обеспечения международной кибербезопасности, научно-исследовательскую основу которой составляют работы следующих авторов: Касеновой М. Б [[5]](#footnote-5) , Кардавы Н.В[[6]](#footnote-6), Капустина А.Я[[7]](#footnote-7).

Большое число теоретических и практических исследований российских авторов в области информационной безопасности и кибербезопасности посвящено вопросам использования информационно-коммуникационных технологий в военно-политических целях. В данной работе были использованы работы Паршина С. А, Горбачева Ю. Е, Кожанова Ю. А[[8]](#footnote-8), Гриняева С. Н[[9]](#footnote-9), Макаренко С.И[[10]](#footnote-10), Макарова В.Е[[11]](#footnote-11), Бухарина С.Н. и Цыганова В.В[[12]](#footnote-12), Мкртычяна А.А[[13]](#footnote-13), Сулеймановой Ш.С. и Назаровой Е.А[[14]](#footnote-14), Шелкоплясовой Н.И[[15]](#footnote-15).

Современные информационные технологии часто становятся источником киберугроз и киберопасностей, для анализа новейших информационных технологий в данной работе использованы работы Душкина Р.В[[16]](#footnote-16), Потапова А.С[[17]](#footnote-17), Мурзина Ф.А., Батура Т.В., Семич Д.Ф[[18]](#footnote-18), Калашникова А.О., Аникиной Е.В[[19]](#footnote-19), Запечникова С.В[[20]](#footnote-20), Цветкова В.Я[[21]](#footnote-21).

**Источниковую базу** исследования составляют следующие документы:

1. Нормативно-правовые документы Российской Федерации и современных государств: федеральные законодательные акты; национальные стратегии кибербезопасности и информационной безопасности; военные доктрины и стратегии по ведению операций в киберпространстве.

2. Официальные документы международных организаций, таких как: Африканский союз, Европейский союз, Организация американских государств, Организация по безопасности и сотрудничеству в Европе, Региональный форум Ассоциации государств Юго-Восточной Азии, Совет Европы, Организация Объединенных Наций, Организация Североатлантического договора, Международный союз электросвязи, Шанхайская организация сотрудничества.

3. Аналитические материалы организаций, специализирующихся на вопросах информационной безопасности: Kaspersky, McAfee, T-Adviser.

**Основной целью** данной работы является определение места и роли киберугроз и киберопасностей в системе национальной безопасности современных государств.

**Объектом** исследования выступает система национальной безопасности современных государств.

**Предметом** исследования является место и роль киберугроз и киберопасностей в системе национальной безопасности современных государств.

Для достижения указанной цели, в работе поставлены и решаются **задачи:**

1. Выделить основные подходы к понятиям «киберугроза» и «киберопасность»;
2. Оценить влияние диверсификации цифровой инфраструктуры на состояние кибербезопасности;
3. Определить механизмы регулирования ответственного поведения государств в контексте международной безопасности;
4. Охарактеризовать роль и место киберугроз и киберопасностей в стратегии национальной кибербезопасности США;
5. Охарактеризовать роль и место киберугроз и киберопасностей в системе национальной безопасности КНР;
6. Охарактеризовать роль и место киберугроз и киберопасностей в национальных стратегиях кибербезопасности государств Евросоюза;
7. Охарактеризовать роль и место информационной безопасности в обеспечении суверенитета Российской Федерации;
8. Экспонировать основные законодательные акты, определяющие статус киберугроз и киберопасностей в Российском информационном пространстве;
9. Оценить перспективы защиты Российской Федерации от иностранных информационных интервенций.

**Методологическую основу исследования** составляют методы научного познания, используемые в современной политической науке. Для выявления и анализа нормативно-правовых аспектов в области обеспечения безопасности в киберпространстве использовался институциональный подход. Системный подход позволил представить политику кибербезопасности современных государств в целостном виде, состоящей из взаимосвязанных элементов. Сравнительный подход был использован для выявления различий и точек соприкосновения позиций государств в обеспечении кибербезопасности, в особенности в контексте международной безопасности. Исторический анализ, позволил описать эволюцию подходов современных государств к обеспечению кибербезопасности, и сущности киберугроз и киберопасностей. Описательный метод использовался для раскрытия содержания киберугроз и киберопасностей. С помощью метода «case study» был проведен анализ примеров деструктивного использования информационно-коммуникационных технологий. Методы статистического анализа позволили проанализировать динамику инцидентов в киберпространстве, а также динамику информатизации Российской Федерации.

**Практическая и теоретическая значимость исследования** заключается в возможности его использования в политико-аналитической деятельности. Проведенный анализ механизмов обеспечения кибербезопасности и законодательств ведущих мировых держав в области информационной безопасности и кибербезопасности, может быть учтен при разработке российских доктрин, стратегий и законодательных актов.

Проведенный комплексный анализ политики обеспечения кибербезопасности, также демонстрируют расстановку политических сил в глобальном информационном пространстве.

**Структура** выпускной квалификационной работы включает введение, три главы, заключение, список использованной литературы.

Первая глава состоит из трех параграфов, в первом из которых представлены основные подходы к понятиям «киберопасность» и «киберугроза», во втором рассматривается диверсификация цифровой инфраструктуры как фактор современных опасностей и угроз, а в третьем – регулирование ответственного поведения государств в контексте международной безопасности.

Вторая глава состоит из трех параграфов: в первом рассматривается киберугрозы в стратегии национальной безопасности США, во втором – угрозы и вызовы в сфере кибербезопасности в государственных программах и стратегиях КНР, а в третьем киберугрозы в стратегиях кибербезопасности государств Евросоюза.

Третья глава состоит из трех параграфов: в первом рассматривается роль информационной безопасности в обеспечении суверенитета России, во втором – опасности и угрозы в киберпространстве в нормативных документах Российской Федерации по обеспечению информационной безопасности, а в третьем - перспективы защиты России от иностранных информационных интервенций и кибервоздействий.

#

# **Глава 1. КИБЕРБЕЗОПАСНОСТЬ КАК СОСТАВЛЯЮЩАЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ**

# **1.1 Основные подходы к понятиям «киберопасность» и «киберугроза»**

Ускоренное развитие информационных технологий за последние 30 лет значительно изменило мир в самых различных сферах. Глобальная информатизация общества является одной из доминирующих тенденций развития человеческой цивилизации в XXI в. Стремительное развитие информационных технологий, увеличение возможностей телекоммуникационных систем приводит к появлению новых вызовов и угроз, совершаемых в киберпространстве[[22]](#footnote-22). В настоящее время можно отметить значительный среднегодовой рост числа инцидентов в области информационной безопасности, затрагивающие широкий спектр частных корпоративных, а также государственных интересов. Сложившаяся ситуация предполагает повышение значимости кибербезопасности в системе информационной безопасности. Основные термины, относящиеся к сфере кибербезопасности, такие как «кибербезопасность», «киберпространство», «киберугроза», «киберопасность» во многом схожи с терминами «информационная безопасность», «информационное пространство», «информационная угроза», «информационная опасность». Таким образом, для того чтобы дать определение понятиям кибербезопасности, в первую очередь необходимо рассмотреть термины, относящиеся к информационной безопасности, чтобы отделить первые от вторых.

Понятие «информационное пространство» в российском научном сообществе было впервые использовано О.В. Кедровским в работе «Информационное пространство России» [[23]](#footnote-23) . В последствии оно рассматривалось в трудах С.А. Модестова, И.М. Дзялошинского, А.С. Чупрова, Н.Б. Зиновьевой, Е.М. Паленой, С.Э. Зуева. Прежде всего, для определения понятия «информационное пространство» следует рассмотреть основополагающие термины «информация» и «пространство». В Федеральном законе РФ № 149 «Об информации, информационных технологиях и о защите информации» от 3 апреля 2005 г. под информацией понимаются сведения (сообщения, данные) независимо от формы их представления[[24]](#footnote-24). В Философском словаре под редакцией Фролова И.Т. под термином «пространство» подразумевается — понятие, которое характеризует взаимное расположение сосуществующих объектов» [[25]](#footnote-25). Следовательно, объединив два понятия, «информационное пространство» может быть определено как взаимодействие субъектов и объектов окружающей среды, связанных процессами производства и потребления сведений.

В работе Дзялошинского И.М. «Информационное пространство России: структура, особенности функционирования, перспективы эволюции» проведен анализ основных подходов к определению понятия «информационное пространство», выделяя при этом «геополитический»; «социальный»; «ноосферно-информационный» подходы[[26]](#footnote-26).

 С точки зрения геополитического подхода, под информационным пространством понимается некая виртуальная территория, принадлежащая государству, которая является своего рода государственным ресурсом и должна быть защищена от внешних посягательств. субъектом территория. Отличительным признаком данного вида информационного пространства является наличие границ. В рамках этого пространства располагаются информационные ресурсы, источники информации, различные технические устройства, обрабатывающие информацию, пользователи информационных ресурсов, которые в свою очередь подпадают под юрисдикцию законодательства, действующего на территории данного государства.

Согласно социальному подходу информационное пространство является сферой отношений между людьми с целью обмена информацией. Информационное пространство рассматривается, как общность определенных структур, взаимодействующих на основе информационных отношений. Например, в работе Лихтина А.А. и Ковалева А.А. информационное пространство определено как составная часть социального пространства, в частности его политической составляющей[[27]](#footnote-27).

Ноосферно-информационный определяет информационное пространство как некую никому принадлежащая совокупность информационных ресурсов, средств обеспечения их пополнения и обработки, а также механизмов доступа пользователей к этим ресурсам.

В современной отечественной науке определение актуальных проблем информационной безопасности стало предметом комплексных исследований, проведенных Лазаревым И.А[[28]](#footnote-28), Лопатиным В.Н.[[29]](#footnote-29), Уфимцевым Ю.С. и Ерофеевым Е.А[[30]](#footnote-30).

В работе Чеботарёвой А.А. рассмотрены основные научные подходы к определению понятия «информационная безопасность». Философский подход основан на выделении трех составляющих: удовлетворение информационных потребностей субъектов; обеспечение безопасности информации; обеспечение защиты субъектов[[31]](#footnote-31). Информационная безопасность, представляет из себя такое состояние объекта, при котором состояние информационной среды, позволяет сохранять способность и возможность принимать и реализовывать решения сообразно целям объекта[[32]](#footnote-32).

Технический подход сосредоточен в первую очередь на проблеме разработки стандартов безопасности, включающих защиту серверов, лицензирование, сертификацию и аттестацию объектов информатизации, применение криптографических систем при передаче данных по каналам связи и других механизмов защиты информации[[33]](#footnote-33).

В социологии информационная безопасность рассматривается в рамках социологии информатики - одного из направлений социологии.

В юриспруденции также отсутствует единый подход к определению понятия «информационная безопасность». Лопатин В.Н. дает определение информационной безопасности как состояние защищенности жизненно важных интересов личности, общества и государства от негативного информационного воздействия[[34]](#footnote-34). Стрельцов А.А. считает, что обеспечение информационной безопасности представляет сложный процесс, который включает в себя объект безопасности, состоящий из совокупности информационных потребностей государства, деятельности по удовлетворению этих потребностей, угроз объекту безопасности, процесс противодействия угрозам[[35]](#footnote-35).

В доктрине информационной безопасности Российской Федерации приведено понятие «информационная угроза» определено как совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере [[36]](#footnote-36).

В стратегических документах и законодательных актах Российской Федерации используется различная терминология для обозначения сети Интернет или информационного пространства[[37]](#footnote-37). Такие различия, в терминологическом употреблении и правовом значении, во многом обусловлены релевантностью их перевода на национальный язык[[38]](#footnote-38). Тем не менее, в отечественной и зарубежной литературе, а также в нормативно правовых актах разных стран, все чаще встречается термины, содержащие приставку «кибер» [[39]](#footnote-39), значение которой скрывается за термином «кибернетика» - (от греч. «искусство управления») - наука об общих закономерностях процессов управления и передачи информации в машинах, живых организмах и обществе[[40]](#footnote-40).

Вокруг киберпространства ведутся активные дискуссии уже значительный период времени, однако однозначной трактовки этого понятия нет. Однозначная интерпретация термина киберпространства невозможна по трем причинам. Первая - отождествление киберпространства и пространства интернета. Вторая - подмена понятий киберпространства и виртуальной реальности. Третья – высокая скорость разработки, внедрения и распространения новейших технологий создает серьезные препятствия для осуществления актуального анализа. Уэллман Б. в своей работе «Physical place and cyberplace: the rise of personalized networking» рассматривает киберпространство в качестве инструмента организации реального мира, которое также становится местом обитания людей и сосуществует наряду с физическим пространством, которое продолжает сохранять свое важное значение[[41]](#footnote-41).

Войскунский А.Е. под киберпространством подразумевает пространство, которое содержит практически неограниченные объемы информации, имеющее конечные размеры, которые могут быть измерены с помощью каких либо метрик[[42]](#footnote-42).

С точки зрения физического или материального восприятия киберпространства, важным является наличие определенных устройств, посредством которых киберпространство создается и функционирует. Киберпространство – это виртуальное место, создаваемое сетью взаимосвязанных компьютеров, в котором взаимодействуют агенты[[43]](#footnote-43).

Для понимания содержания терминов киберугроза и киберопасность, целесообразно обратится к понятиям «опасность» и «угроза». Опасность – объективно существующая возможность негативного воздействия на некий объект, в результате которого ему может быть причинении ущерб, вред, ухудшающий его состояние, предающий его развитию негативную динамику[[44]](#footnote-44). Угроза – опасность, на стадии готовности перейти из возможности в действительность[[45]](#footnote-45). Следовательно, в самом широком смысле можно определить термин «киберугроза» как совокупность условий и факторов, характеризуемое реальной возможностью нарушения кибербезопасности, путем незаконного вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных целей. Термин «киберопасность» соответственно, как совокупность условий и факторов, при определенных условиях способных привести к возникновению киберугрозы. Стоит отметить, что международное сообщество до сих пор не пришло к единому пониманию ключевых терминов в области кибербезопасности. Можно выделить два основных подхода к определению кибербезопасности: широкий подход и узкий подход. В рамках широкого подхода понятие кибербезопасности включает в себя как технические, так и психологические аспекты. Узкий подход, ограничивается исключительно техническими аспектами. К примеру, в стратегии кибербезопасности Швеции под кибербезопасностью понимается комплекс мер безопасности, направленных на сохранение конфиденциальности, достоверности и доступности информации[[46]](#footnote-46). В свою очередь Германия в стратегии кибербезопасности использует узкий подход, где кибербезопасность определена как желаемая цель информационной безопасности, ситуация, в которой риски немецкого киберпространства были уменьшены до приемлемого минимума[[47]](#footnote-47).

В некоторых научных работах, киберугрозы и киберопасности рассматриваются как совокупности угроз и опасностей информационной безопасности. Г. Кершишниг, в своем исследовании[[48]](#footnote-48), посвященном проблеме киберугроз, использует ряд терминов, обозначающие различную степень опасности для информационной безопасности. В частности, им приведены термины: «кибервмешательство» – наиболее общий понятие; «киберинцидент» - происшествия в киберпространстве оставшиеся без наказания; «кибератака» - любая попытка деструктивного воздействия на устройство; кибервойна – противоборство и противостояние в киберпространстве[[49]](#footnote-49). Совокупность перечисленных терминов, в данном случае, будет обозначена как «киберугрозы».

В международном стандарте ISO 27032, который выполнен в стиле риск-ориентированного подхода, и который определяет активы киберпространства и заинтересованные стороны, угрозы, рекомендации и меры по обработке рисков, киберпространство формулируется как комплексная виртуальная среда, сформированная в результате действий людей, программ и сервисов в сети Интернет посредством соответствующих сетевых и коммуникационных технологий. По аналогии с классическим определением информационной безопасности в стандарте под кибербезопасностью фактически понимают свойство защищенности активов от угроз конфиденциальности, целостности, доступности в киберпространстве. В стандарте не дается определения киберугроз, однако, на основании приведенной в стандарте схемы «Основные понятия кибербезопасности и связь между ними», можно сделать вывод, что киберугроза – использование агентами киберугрозы уязвимостей информационной системы, для неправомерного использования или повреждения активов информационной системы. В документе также присутствует понятие «Риск» кибербезопасности, которое может быть определено как степень вероятности возникновения киберугроз[[50]](#footnote-50).

Термины «кибербезопасность», «киберопасность» и «киберугроза» в специальной литературе могут использоваться в контексте безопасности составных частей киберпространства. К примеру, в работе Зубарева И.В., Жидкова И.В. и Кадушкина И.В., кибербезопасность автоматизированных систем управления (далее АСУ) военного назначения. Под кибербезопасностью АСУ в работе понимается состояние защищенности хранящейся, обрабатываемой и передаваемой в АСУ военного назначения информации от угроз информационно-технического характера. Термин «киберугроза», определен как совокупность условий и факторов определяющую информационно-техническое воздействие на информацию или состояние АСУ, ее объекты или среду функционирования, которые могут привести к недопустимому ущербу или неспособности выполнения АСУ своих функций[[51]](#footnote-51). Такой подход может использоваться для рассмотрения кибербезопасности всех составных частей киберпространства.

Периодически, термин «киберугроза» употребляется в контексте информационной безопасности, являясь синонимичным понятию «угроза информационной безопасности» [[52]](#footnote-52). При подобном подходе, важно учитывать соотношение понятий «кибербезопасность» и «информационная безопасность», всякая киберугроза будет являться угрозой информационной безопасности, но не всякая угроза информационной безопасности будет являться киберугрозой.

Таким образом, поскольку в научной среде нет единого определения терминов «киберпространство», «кибербезопасность», «киберопасность» и «киберугроза», также нельзя выделить какой-либо из рассмотренных подходов к определению данных терминов, который отражал бы полностью суть этих понятий, то в последующей работе в качестве основного определения указанных терминов будут использованы следующие формулировки: киберпространство - пространство, создаваемое сетью взаимосвязанных компьютеров, которое содержит практически неограниченные объемы информации; кибербезопасность - желаемая цель состояния киберпространства, в которой угрозы и опасности сведены до приемлемого минимума; киберугроза - совокупность условий и факторов, характеризуемое реальной возможностью нарушения кибербезопасности, путем незаконного вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных целей; киберопасность - совокупность условий и факторов, при определенных условиях способных привести к возникновению киберугрозы.

# **1.2 Диверсификация цифровой инфраструктуры как фактор современных киберугроз и киберопасностей**

Настоящий период развития Российской Федерации, напрямую связан с процессами цифровизации, связанными, прежде всего с развитием и внедрением информационных технологий в различные сферы жизни российского общества[[53]](#footnote-53). Утвержденные российским правительством национальные проекты в таких сферах как: здравоохранение, образование, наука, цифровая экономика и ряда других, создают основу для разработки, создание и внедрение современных информационных технологий практически во все направления деятельности российского государства [[54]](#footnote-54).

Развитие экономики Российской Федерации в настоящее время невозможно без развитой в достаточной степени информационной инфраструктуры. Согласно доктрине информационной безопасности Российской Федерации, информационная инфраструктура - совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации[[55]](#footnote-55). Наибольшее значение для современной экономики представляют следующие составляющие цифровой инфраструктуры: центры обработки данных, сервисы облачных вычислений, цифровые платформы, услуги с использованием новых цифровых технологий— аналитики данных, искусственного интеллекта. Предоставление повсеместного широкополосного доступа, в особенности с использованием интеллектуальных мобильных устройств является основополагающей технологической тенденцией[[56]](#footnote-56). В российской экономике информационные технологии и информационные услуги стали значимой статьей не сырьевого экспорта, так в период с 2000 по 2010 год отрасль информационных технологий развивалась высокими темпами с ежегодным приростом около 25 процентов[[57]](#footnote-57). По данным государственной программы Российской Федерации «Информационное общество (2011 - 2020 годы)», утвержденной распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р, на период начала программы, только 34 процента российских домашних хозяйств имели широкополосный доступ в сеть Интернет, доля органов государственной власти и местного самоуправления, имевших скорость передачи данных через  информационно телекоммуника­ционную сеть "Интернет" не менее 2 Мбит/сек составляла 22 процента, то к 2019 году, число российских домашних хозяйств имеющих широкополосный доступ в сеть Интернет выросло до 75% , а доля органов государственной власти и местного самоуправления, имевших скорость передачи данных через  информационно телекоммуника­ционную сеть "Интернет" не менее 2 Мбит/сек составила 85 % [[58]](#footnote-58). Учитывая всестороннее развитие цифровой инфраструктуры Российской Федерации, уместно говорить о происходящих в ней процессах диверсификации.

Подходы к определению термина «диверсификация» претерпевали изменения в результате исторического развития, но однозначного подхода не существует и по настоящее время, однако в контексте диверсификации цифровой инфраструктуры, целесообразно использовать определение, приведенное в работе Гуцева М.В., диверсификация – расширение видов деятельности , проникновение в новые отрасли[[59]](#footnote-59). Шишкина Т. С. Пишет, что диверсификация является одним из важнейших инструментов развития, так как позволяет более результативно использовать возможности предприятия или организации[[60]](#footnote-60).

В результате, современная цифровая инфраструктура включает в себя: информационные центры, сети подвижной сотовой связи, подсистемы, банки данных и знаний, системы связи, центры управления, аппаратно-программные средства и технологии обеспечения сбора, хранения, обработки и передачи информации, центры обработки данных, сервисы облачных вычислений, цифровые платформы, услуги с использованием новых цифровых технологий— аналитики данных, искусственного интеллекта, технологии блокчейн[[61]](#footnote-61).

Цифровая инфраструктура рассматривается в различных сферах жизни российского общества. Цифровой сектор экономики, включает секторы ИКТ, производства контента и СМИ. В секторе государственного управления цифровая инфраструктура реализована прежде всего в направлениях государственного управления и регулирования, мобилизации и подготовки человеческого капитала, цифровых услуг, открытого правительства. В социальной сфере цифровая инфраструктура представлена: в медицине, в направлениях государственной политики в области здравоохранения, подготовки специалистов, национальные базы данных здравоохранения, цифровые медицинские технологии, система телемедицинских консультаций; в образовании в направлениях дистанционного образования, подготовки специалистов, цифровых образовательных ресурсов, образовательных платформ; в культуре, в форме цифровых платформ в сфере культуры, подготовки специалистов культурного сектора, электронных каталогов, виртуальных музеев.

Однако, следует учитывать различного рода риски и угрозы, возникающие при широкомасштабном развитии и распространении информационных технологий. К настоящему времени, вопросы безопасности функционирования информационных технологий стоят в одном ряду с вопросами их эффективности. Говоря о безопасности цифровой инфраструктуры, необходимо рассмотреть составные части цифровой инфраструктуры и определить перечень угроз, скрытых за ними.

Составляющие части цифровая инфраструктуры могут быть разделены на следующие группы, согласно соответствующим им современным информационным технологиям:

1. Квантовые технологии;
2. Технологии искусственного интеллекта;
3. Облачные технологии;
4. Технологии больших данных;
5. Технологии киберфизических систем.

В настоящее время, современные квантовые технологии можно разделить по следующим направлениям[[62]](#footnote-62):

1. Квантовые компьютеры;
2. Квантовая сенсорика;
3. Квантовая связь;
4. Квантовые вычисления.

Квантовая передача данных или квантовая связь, в настоящее время является наиболее развитым направлением квантовых технологий, так как уже созданы и активно эксплуатируются квантовые каналы связи, защищающие передачу от большого числа «традиционных» атак. Вместе с тем большая часть квантовых протоколов распределения ключей на практике сталкивается с определенными техническими проблемами, что позволяет осуществлять некоторые специализированные атаки на квантовые каналы связи[[63]](#footnote-63).

Под квантовой сенсорикой понимается создание сенсоров, датчиков, измерительных приборов, основанных на квантовых эффектах. Планируется, что квантовые сенсоры, будут обладать высоким пространственным и временным разрешением, что позволит значительно увеличить точность и частоту измерений произвольных свойств заданных объектов[[64]](#footnote-64).

Квантовые вычисления и, необходимый для их реализации, квантовый компьютер находятся в стадии разработки прототипа. Квантовые вычисления достаточно глубоко проработаны теоретически, однако, реализовать данную вычислительную модель на традиционной архитектуре современных компьютеров невозможно. На текущий момент имеется информация только о прототипах с числом кубитов порядка 72[[65]](#footnote-65). Этого числа кубитов недостаточно, чтобы реализовать какой-либо полноценный квантовый алгоритм.

Полноценный квантовый компьютер позволит решать задачи самых различных направлений, начиная от дешифровки криптографических систем, заканчивая моделированием и симуляцией квантовых систем произвольного уровня сложности. С точки зрения киберугроз, квантовый компьютер в значительной степени затронет область криптографии, с одной стороны дискредитируя существующие системы защиты информации, а другой стороны парируя эти угрозы механизмами квантовой криптографии.

Термин «искусственный интеллект» используется для обозначения большого направления научных и прикладных исследований. Исследователи выделяют две основные цели своей работы – это создание компьютерных моделей, имитирующих процессы решения человеком тех или иных интеллектуальных задач, и автоматизация интеллектуального направления человеческой деятельности.

Сфера искусственного интеллекта довольно неоднородна. В ней существуют различные направления исследований, которые различаются или задачей, требующей интеллектуального анализа, или используемыми инструментами, или развитой моделью мышления. Сферы, определенные на основе решенной проблемы, включают[[66]](#footnote-66):

* 1. машинный перевод;
	2. автоматическое реферирование и информационный поиск;
	3. системы речевого общения;
	4. игровой интеллект, доказательство теорем и автоматизация научных исследований;
	5. компьютерное зрение;
	6. извлечение данных.

Технологии искусственного интеллекта, сами по себе, не расширяют пространство киберугроз для информационной инфраструктуры, тем не менее, они в значительной степени влияют на эффективность различного рода кибератак, исходящих от связанных с ними технологий.

Под облачными технологиями, как правило, понимается предоставление пользователю компьютерных ресурсов и мощностей в виде интернет-сервисов. При это, пользователь может не иметь информации о том, какие вычислительные машины обрабатывают его запросы, какая при этом используется операционная система. Вычислительные облака состоят из тысяч серверов, размещенных в центрах обработки данных. Они единовременно обеспечивают миллионы пользователей необходимыми вычислительными мощностями[[67]](#footnote-67).

Учитывая, что облачные технологии, как правило, используются для хранения, передачи данных, а также или выполнения вычислительных задач, они значительно расширяют спектр киберугроз информационно й инфраструктуры, особенно в части конфиденциальности информации и доступности информационных ресурсов[[68]](#footnote-68).

Общепринятой терминологии в области обработки больших данных еще не сложилось. Однако, термину «большие данные» можно дать следующее определение - это массивы данных такого объема и структуры, которые превышают возможности традиционных программных инструментов по сбору, хранению и обработке данных за приемлемое время. При этом данные могут быть структурированными, слабоструктурированными и неструктурированными, что не позволяет эффективно управлять ими и обрабатывать традиционным образом[[69]](#footnote-69).

Проблема обеспечения безопасности больших данных заключается в противоречии между возрастающими потребностями в обработке таких данных с одной стороны, и недостаточными возможностями гарантировать конфиденциальность, целостность, доступность обрабатываемых данных и компонентов инфраструктуры с другой. Проблемы обеспечения кибербезопасности вызывают необходимость выработки принципиально иных подходов, базирующихся на концепции защиты распределенной, крупномасштабной вычислительной среды больших данных, а не единой физической сущности[[70]](#footnote-70).

Киберфизическая система – представляет собой сложную распределенную систему, управляемую или контролируемую компьютерными алгоритмами, тесно интегрированную с Интернетом и его пользователями, где физические и программные компоненты тесно взаимосвязаны[[71]](#footnote-71).

Также, следует отдельно рассмотреть объекты информационной инфраструктуры, представляющие особенную значимость в системе обеспечения национальной безопасности Российской Федерации, так называемую критическую информационную инфраструктуру. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" подчеркивает важность обеспечения безопасности критической информационной инфраструктуры Российской Федерации. Согласно закону, критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов[[72]](#footnote-72). В свою очередь, объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. Критическая информационная инфраструктура Российской Федерации представлена в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сферы, топливно-энергетического комплекса, атомной энергии, оборонного комплекса, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности, химической промышленности. В зависимости от соответствия критериям значимости объекту критической информационной инфраструктуры присваивается одна из трех категорий значимости. Категорирование осуществляется исходя из[[73]](#footnote-73):

 1) социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

2) политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

3) экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;

4) экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;

5) значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

Подводя итог, можно сделать вывод, что происходящие в Российской Федерации процессы диверсификации цифровой инфраструктуры, приводят к проникновению последней в различные сферы жизни российского общества, в частности в экономику, в сферу государственного управления, в культурный сектор, а также в критические инфраструктуры Российской Федерации, что ввиду новизны таких технологий, несомненно расширяет перечень потенциальных угроз для национальной безопасности России в целом. Приведенные выше анализ процесса диверсификации информационной инфраструктуры позволяет сделать вывод, что, хотя не все современные информационные технологии и процессы информационной трансформации, происходящие в современном российском государстве, неизбежно расширяют перечень киберугроз, это положение остается верным для большинства из них.

# **1.3 Регулирование ответственного поведения государств в киберпространстве в контексте международной безопасности**

Технологическим феноменом настоящего этапа развития человеческого общества, влияющим на жизнедеятельность человека и моделирующим образ мира в целом, является интернет - сложная информационно-техническая система, включающая в себя как технический, так и социальный компонент[[74]](#footnote-74). Расширение сфер применения интернета диверсифицирует правовое регулирование значительного числа общественных отношений как на национальном, так и на международном уровне, а также вызывает необходимость правового регулирования новых общественных отношений[[75]](#footnote-75).

Таким образом, успех каждой отдельно взятой страны по защите своих национальных интересов в информационном пространстве и обеспечению безопасности критической инфраструктуры, в настоящее время зависит от усилий всего мирового сообщества по созданию безопасного киберпространства[[76]](#footnote-76).

Важность сотрудничества всех заинтересованных сторон в формировании норм и правил, регулирующих информационные отношения, признана в ряде международных документов.

Декларация принципов управления Интернетом, принятая Советом Европы в 2011 г., содержит ссылки на документы Всемирного саммита по информационному обществу— Женевскую декларацию принципов 2003 г.9 и Тунисское обязательство 2005 г.10, тем самым признавая важность сотрудничества государств, частного сектора и гражданского общества в вопросах согласования принципов, норм и правил управления Интернетом.

В документе перечислены десять базовых принципов управления Интернетом[[77]](#footnote-77):

* права человека, демократия и верховенство права;
* многосторонняя модель управления;
* ответственность государств;
* привлечение Интернет-пользователей к процессу принятия решений;
* универсальность Интернета;
* целостность Интернета;
* децентрализованное управление;
* соблюдение сетевой архитектуры;
* сетевая открытость;
* культурное и языковое разнообразие

Вопрос о регламентировании действий государств в сфере информационных технологий в рамках ООН, впервые был внесен в повестку дня в декабре 1998 г., когда по инициативе Российской Федерации, была начата дискуссия по международной информационной безопасности.

Важным результатом дискуссии по международной информационной безопасности стало создание в 2004 году группы правительственных экспертов информатизации и телекоммуникационных технологий, что представляло собой значительный шаг для обеспечения международного сотрудничества в данной сфере. Основными задачами группы были определены:

1. Рассмотрение существующих и потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению;
2. Проведение экспертами исследования различных концепций, которые должны укрепить систему безопасности информационных и телекоммуникационных систем[[78]](#footnote-78).

Новым этапом данной дискуссии, стало принятие в 2018 году резолюции А/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». Данная резолюция содержит два принципиально важных момента[[79]](#footnote-79).

Во-первых, она является первоначальным сводом из 13 правил, норм и принципов поведения государств в информационном пространстве.

Положения данной резолюции, включают в себя следующие обязательства[[80]](#footnote-80):

- использовать информационно-коммуникационные технологии исключительно в мирных целях;

- соблюдать в информационном пространстве принцип государственного суверенитета;

- сотрудничать в борьбе с применением информационно-коммуникационных технологий в преступных и террористических целях;

- предотвращать распространение скрытых вредоносных функций в ИТ-продукции.

Также, в указанном своде норм были зафиксированы следующие принципы[[81]](#footnote-81):

- Обвинения в неправомерном использовании информационно-коммуникационных технологий должны быть доказаны;

- Государства не должны привлекать третьих лиц для неправомерного использования информационно-коммуникационных технологий;

- ООН должна принадлежать ведущая роль в международной дискуссии по международной информационной безопасности;

- Суверенитет государств, международные нормы и принципы, проистекающие из суверенитета, применяются к осуществлению государствами деятельности, связанной с информационно-коммуникационными технологиями, и к их юрисдикции над ИКТ-инфраструктурой, расположенной на их территории;

- Государства несут главную ответственность за поддержание безопасной и мирной информационно-коммуникационной среды;

- Государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере информационно-коммуникационных технологий.

Также в нее вошел призыв к Генассамблее создать рабочую группу по международной информационной безопасности открытого состава, в которой смогут участвовать все государства, входящие в состав ООН[[82]](#footnote-82). Это положение, значительно демократизирует переговорный процесс по международной информационной безопасности, и делает его максимально открытым и доступным даже для стран с развивающейся или отсталой информационно-коммуникационной инфраструктурой[[83]](#footnote-83).

На той же сессии ГА ООН, была предложена резолюция США A/RES/73/266 «Поощрение ответственного поведения государств в киберпространстве в контексте международной̆ безопасности». В документе подчеркивается важность существования группы правительственных экспертов, и дается положительная оценка деятельности группы за 2010, 2013 и 2015 годы.

Авторы призывают к созданию в 2019 году новой группы правительственных экспертов на основе справедливого географического распределения и просят управление по вопросам разоружения секретариата, от имени группы правительственных экспертов, сотрудничать с такими региональными организациями как Африканский союз, Европейский союз, Организация американских государств, Организация по безопасности и сотрудничеству в Европе и Региональный форум Ассоциации государств Юго-Восточной Азии[[84]](#footnote-84).

Группа американского варианта, обязана проводить исследования всевозможных совместных мер по защите от имеющихся и перспективных киберугроз, и участвовать в разработке норм и правил по ответственному поведению в киберпространстве.

Вопреки тому, что Российская и Американская резолюции во многом являются конкурирующими друг с другом, создавая при этом дополнительные сложности для осуществления конструктивного сотрудничества в области международной информационной безопасности, серьезных препятствий для осуществления дискуссии нет. Оба документа, положительно оценивают предыдущие результаты работы группы правительственных экспертов, подчеркивают важность участия бизнес сообщества и научных кругов для обеспечения международной информационной безопасности[[85]](#footnote-85).

# **Глава 2. КИБЕРОПАСНОСТИ И КИБЕРУГРОЗЫ В СТРАТЕГИЯХ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ГОСУДАРСТВ**

# **2.1 Стратегия национальной кибербезопасности США «Об основных киберугрозах»**

Соединенные Штаты исторически стали одной из первых стран, которые стали рассматривать кибербезопасность как вопрос стратегического значения. Основные положения стратегии кибербезопасности США сформированы в 1990-е годы. Администрация президента Билла Клинтона в 1995 году обнародовала Стратегию национальной безопасности, в который обозначена задача по достижению информационного превосходства путем наступательных и оборонительных информационных операций[[86]](#footnote-86).

Директива Президента № 63 «О защите критической инфраструктуры», дальнейшее развитие получила в форме кодификациии в «Национальной стратегии безопасности киберпространства»[[87]](#footnote-87) и в Директиве Президента в области национальной безопасности №7 «Об определении, приоритизации и защите критически важных элементов инфраструктуры»[[88]](#footnote-88). В этих документах определены основные принципы и задачи обеспечения кибербезопасности: предотвращение кибератак против критических инфраструктур; ликвидация уязвимостей критических инфраструктур; минимизация потенциального ущерба в случае успешной кибератаки. Также обозначена возможность применения Соединенными Штатами кибероружия, в качестве оборонительной меры.

В 2008 г. создана «Комплексная национальная инициатива кибербезопасности». Данная инициатива предполагала решение ряда задач обеспечения кибербезопасности США[[89]](#footnote-89):

1. Защита национальных баз данных от атак потенциальных противников.

2. Обеспечение информированности специалистов федерального правительства о наличии уязвимостей и угрозах безопасности в национальных компьютерных сетях и критических инфраструктурах.

3. Расширение технических и оперативных возможностей контрразведывательных органов США.

4. Создание системы подготовки специалистов в сфере кибербезопасности.

В 2017 году, подразделение киберкомандования ВС США преобразовано в подразделение стратегического командования[[90]](#footnote-90). Пентагон предоставил киберкомандованию США возможность применять более жесткий подход в отношении не только защиты от хакерских атак, но и вторжений в киберпространства других государств. Ведомству предоставлены полномочия по нанесения превентивных кибератак на цифровые инфраструктуры противников. При этом, действия по защите США от кибератак должны преимущественно происходить в киберпространстве противника. Примером реализации превентивного подхода в обеспечении кибербезопасности является инициатива киберкомандования США по внедрению вредоносного ПО в киберпространство противника[[91]](#footnote-91).

В сентябре 2018 г. президент Дональд Трамп подписал Национальную киберстратегию США. При этом документ 2018 г. во многом повторяет предыдущие документы США в области кибербезопасности.

Национальная киберстратегия выделяет активных противников США, осуществляющих свою деятельность в киберпространстве. В частности, отмечается, что Россия, Иран, Северная Корея и Китай совершают кибератаки, которые наносят ущерб американской и международной экономике, а также осуществляют акты экономического шпионажа за США и их союзниками[[92]](#footnote-92).

Стратегия национальной кибербезопасности состоит из 4 частей, каждой из которых соответствует определенное направление политики США:

1. Protect the American People, the Homeland, and the American Way of Life;
2. Promote American Prosperity;
3. Preserve Peace through Strength;
4. Advance American Influence.

В первой части «Protect the American People, the Homeland, and the American Way of Life» обозначена цель - обеспечение надлежащего управления рисками в области кибербезопасности, повышение безопасности и защищенности информационных систем и информации, имеющей государственную важность .

Реализация цели первой части, происходит путем защиты федеральных сетей и информации, защиты критически важной инфраструктуры, борьбы с киберпреступностью и улучшения отчетности об инцидентах, включающей в себя предоставление департаменту внутренней безопасности более широких полномочий контроля за гражданскими усилиями в области кибербезопасности, сотрудничество с другими странами в целях борьбы с киберпреступностью. Приведенные в документе угрозы кибербезопасности США могут быть структурированы следующим образом:

1) Нарушение функционирования сетей федеральных департаментов и агентств;

2) Ненадлежащее качество IT продуктов и услуг в системе федеральной системе снабжения США;

3) Ненадежность федеральных подрядчиков, имеющих доступ к государственной тайне;

4) Использование государственными учреждениями устаревших IT продуктов или стандартов;

5) Дестабилизация критической инфраструктуры;

6) Кибератаки на избирательную инфраструктуру, транспортную, морскую и космическую инфраструктуру.

Вторая часть национальной стратегии кибербезопасности США - «Promote American Prosperity» ставит целью сохранить влияние Соединенных Штатов в технологической экосистеме и развивать киберпространство в качестве двигателя экономического роста, инноваций и эффективности.

Реализация цели второй части стратегии предполагает: развитие жизнеспособной и эффективной цифровой экономики; поощрение и защиту изобретательности США; создание квалифицированного кадрового резерва; сотрудничество с IT компаниями, для тестирования кибербезопасности в новых продуктах; привлечение и удержание высококвалифицированных кадров по кибербезопасности. При этом, во второй части киберстратегии представлен ряд мероприятий по обеспечению кибербезопасности США и международной безопасности, среди которых:

1) Создание единых международных стандартов кибербезопасности;

2) Создание стандартов кибербезопасности цифровой инфраструктуры следующего поколения;

3) Экономическая и политическая поддержка IT продуктов в сфере кибербезопасности американского производства;

4) Усиление контрразведывательных мероприятий в области IT технологий;

5) Финансирование программ школьного и университетского IT образования;

В Третьей части «Preserve Peace through Strength» определена цель - выявлять, противодействовать, пресекать, ослаблять интенсивность и сдерживать действия в киберпространстве, которые дестабилизируют и противоречат национальным интересам, сохраняя при этом превосходство США в киберпространстве и посредством него».

Осуществление данной цели предполагается посредством создания норм ответственного поведения государств и сдерживания недопустимого поведения в киберпространстве. В стратегии говорится, что администрация будет использовать «все инструменты национальной власти» для предотвращения кибератак и осуществлять быстрые и эффективные действия против злоумышленников.

Четвертая часть «Advance American Influence» ставит целью сохранить долгосрочную открытость, функциональную совместимость, безопасность и надежность интернета, который поддерживается и усиливается интересами Соединенных Штатов.

Осуществление цели четвертой части стратегии, предполагает: продвижение открытого, международного, надежного и безопасного Интернета; наращивание международного кибер-потенциала; совместное противодействие угрозам, направленным на взаимные интересы.

16 ноября 2018 года президент Дональд Трамп подписал закон «о Агентстве кибербезопасности и защиты инфраструктуры» [[93]](#footnote-93) от 2018 года. Этот закон усиливает роль бывшего Национального управления по защите программам и преобразует его в агентство кибербезопасности и защиты инфраструктуры (CISA). Управлению предоставляются полномочия по созданию национального потенциала для защиты от кибератак и взаимодействию с федеральным правительством по предоставлению инструментов кибербезопасности, служб реагирования на инциденты и возможностей оценки для защиты государственных сетей.

Таким образом, политика США в области киберпространства и кибербезопасности, в первую очередь направлена на достижение информационного превосходства. Наряду с задачами обеспечения безопасности киберпространства, в рассмотренных нормативных документах обозначены политические цели и перечислены основные противники США в киберпространстве - Россия, Китай, Иран, КНДР и международные террористические организации. Указано, что перечисленные акторы используют киберпространство в военных и политических целях, регулярно проводят кибератаки направленные против США и их союзников, при, не приводя каких-либо существенных доказательств.

Военно-политическое руководство США считает, что различного рода кибератаки становятся неотъемлемой частью современных вооруженных конфликтов, киберподразделения функционирующие в рядах вооруженных сил США или в качестве отдельных ведомств, обладают полномочиями к проведению кибератак на виртуальное пространство противника или к проведению мероприятий кибершпионажа за государствами или отдельными гражданами по всему миру, о чем свидетельствует утечка со стороны сотрудника компании-подрядчика агентства национальной безопасности Э. Сноудена, о деятельности агентства по сбору данных и слежению за сетевой и коммуникационной активностью не только граждан США, но и в глобальном масштабе, включая личные коммуникации лидеров государств[[94]](#footnote-94).

Очевидно, что такой, своего рода «наступательный» подход в обеспечении кибербезопасности может стать дестабилизирующим фактором, поскольку приведет к своеобразной гонке кибервооружений и наращиванию киберпотенциала, а упоминание Российской Федерации в стратегии национальной кибербезопасности США как прямого виновника различных инцидентов в американском киберпространстве, создает опасность нанесения США «ответных» кибератак по российской цифровой инфраструктуре.

# **2.2 Государственные программы и стратегии КНР об угрозах и вызовах в сфере кибербезопасности**

#

В 2000 году в Китае было предпринята попытка классификации вероятных правонарушений в информационной сфере, результатом которой явилось «Постановление Всекитайского собрания народных представителей по защите интернет - пространства», где были выделены области, в которых возможны нарушения: экономическая, образовательная, сфера поддержания общественной стабильности и защиты граждан[[95]](#footnote-95). В 2002 году была сформирована и опубликована оборонная политика Китая, в которой делался упор на модернизации вооруженных сил КНР, в частности их информатизации[[96]](#footnote-96).

В 2003 г. было опубликовано «Постановление государственной руководящей группы по работе в области укрепления информационной безопасности». Документ закрепляет за ответственными лицами необходимость предпринимать шаги по укреплению защиты стратегической инфраструктуры, проведению мониторинга интернет-пространства на наличие возможных угроз для КНР, разработке мер для привлечения квалифицированных специалистов в области информационной безопасности[[97]](#footnote-97).

C 2004 года в КНР начата реализация государственной программы «Золотой щит», суть которой заключается в фильтрации интернет трафика между китайским киберпространством и остальным миром. Фактически, программа «Золотой щит» представляет из себя попытку китайского правительства осуществить тотальный контроль за киберпространством, с целью ограничения доступа китайских граждан к зарубежным Интернет-ресурсам, средствам массовой коммуникации и социальным сетям[[98]](#footnote-98).

В 2006 г. была принята «Государственная стратегия по развитию информатизации на период с 2006 по 2020 г.» В данном документе подчеркивается высокая важность контроля информационных технологий. Предполагается создать специальные структуры для регулирования процессов в информационной среде. Предусматривается установление вектора развития информационных технологий и государственной политики в этой области. В стратегии планируется создание собственного программного обеспечения, а также сочетание установки военной и гражданской продукции[[99]](#footnote-99).

Идея суверенной кибербезопасности дальнейшее развитие получила в положениях нового Закона о национальной безопасности, принятого в Китае в 2015 году, подчеркнута необходимость укрепления защиты национальных информационных систем и установления суверенитета киберпространства в Китае. Эти вопросы подробнее рассматриваются в законе о кибербезопасности, который предполагает обязательную регистрацию в интернет-сервисах под настоящими именами, привлечение частных операторов к участию в правительственных расследованиях, введение множества обязательств по хранению персональных данных в Китае, которые должны храниться только в стране. В 2016 году закон был окончательно принят, а в 2017-м году вступил в силу [[100]](#footnote-100).

 Часть содержания закона повторяет существующие правила, принятые Китаем на протяжении многих лет и просто объединяет отдельные нормативные акты в один. Ранее существовавшие правила были разбросаны по разным нормативным актам. Правительство КНР, при принятии данного закона, во многом руководствовалось положением, что формирование единого закона улучшает эффективность правового регулирования киберпространства, в большей мере информирует бизнес-сообщество, а также широкую общественность о беспрецедентных угрозах кибербезопасности в пределах и за пределами границ Китая[[101]](#footnote-101).

В законе дается определение ряду терминов, относящихся к сфере кибербезопасности. Согласно статье 76, кибербезопасность относится к принятию необходимых мер для предотвращения кибератак, вторжений, помех, уничтожения и незаконного использования, с целью обеспечения стабильного, надежного работа и конфиденциального функционирования сети. Сети рассматриваются здесь как системы, состоящие из компьютеров и других информационных устройств или объектов, используемых для “сбора, сохранения, передачи, обмена и обработки информации. Личная информация относится ко всем видам информации, записанной в электронном виде или с помощью других средств, взятой в одиночку или вместе с другой информацией, достаточной для идентификации личности физического лица, включая физических лиц: полные имена, даты рождения, национальные идентификационные номера, личная биометрическая информация, адреса, номера телефонов[[102]](#footnote-102).

В статье 31 закона о кибербезопасности КНР говорится, что государство должно сосредоточиться на вопросах защиты критической информационной,
инфраструктуры в сферах связи с общественностью, предоставления информационных услуг, энергетики, транспорта, водного хозяйства, финансов, государственные услуги, электронного правительства и других ключевых элементов информационной инфраструктуры, нарушение функционирования которой повлечет урон национальной безопасности, национальной экономики и поставит под угрозу жизни граждан[[103]](#footnote-103).

Операторы критической информационной инфраструктуры должны хранить ключевые данные и персональную информацию на территории Китайской Народной Республики. В тех случаях, когда необходимо предоставлять информацию внешним агентам, оценка безопасности
проводится в соответствии с мерами, сформулированными
национальным органом по управлению киберпространством совместно с
соответствующими департаментами Государственного Совета. На операторов сетей возлагаются юридические обязательства в рамках данного закона[[104]](#footnote-104).

Закон также устанавливает основополагающий принцип -
поощрение и защита национального суверенитета в киберпространстве
в рамках сетей. Перечень дополнительных обязательств для операторов сетей включает:

1. соблюдение требований многоуровневой системы защиты
кибербезопасности;
2. аутентификацию реальной личности пользователей;
3. разработку стратегий действия в чрезвычайных ситуациях в области кибербезопасности;
4. оказание помощи и поддержки
следственным органам.

Также, закон регламентирует деятельность интернет СМИ и социальных сетей. Весь произведенный в сети контент сохраняется на территории КНР в течении 6 месяцев. Особое внимание в законе уделяется системе идентификации: для осуществления какой либо деятельности в сети, гражданам Китая необходимо подтвердить свою личность и пройти соответствующую процедуру верификации, иными словами, закон запрещает интернет анонимность[[105]](#footnote-105).

Таким образом, закон о кибербезопасности с одной стороны, защищает объекты критической информационной инфраструктуры КНР от киберугроз, связанных с кражей персональных данных и предостерегает от кибершпионажа, а с другой стороны, предоставляет специальным службам КНР возможность физического доступа к данным объектов критической информационной инфраструктуры. Несмотря на то, что в законе употребляется понятие «угроза кибербезопасности», киберугрозы главным образом рассматриваются в рамках критической информационной инфраструктуры и информационных сетей, и представлены довольно общими определениями, такими как: кража персональных данных, нарушение функционирования и т.д.

Более подробно, киберугрозы представлены в уголовном законодательстве КНР. В соответствии с уголовным законодательством Китайской Народной Республики киберпреступления в основном рассматриваются в разделе: “преступления, связанные с нарушением общественного порядка”. Статьи 285, 286 и 287 являются основными статьями, которые непосредственно касаются киберпреступлений.

Кража или иное приобретение личной информации граждан, рассматривается как “преступление нарушения личной информации гражданина”, предусмотренное в статье 253.

В соответствии со статьей 285 Уголовного кодекса деятельность, связанная с вторжением в компьютерную информационную систему в области государственных дел, национальной обороны или передовой науки и техники, квалифицируется как “преступление, заключающееся во вторжении в компьютерную информационную систему”.  Что касается деятельности по вторжению в компьютерную информационную систему, то она может представлять собой “преступление, связанное с получением данных из компьютерной информационной системы и управлением компьютерной информационной системой”.

Согласно статье 286 Уголовного кодекса, отказ в обслуживании может квалифицироваться как " преступление, связанное с подрывом компьютерной информационной системы”, и в особо тяжких случаях может предусматриваться лишение свободы на срок свыше пяти лет.

Умышленное создание и распространение компьютерных вирусов и иных программ деструктивного характера, оказывающих влияние на нормальное функционирование компьютерных систем, рассматривается в соответствии с частью первой статьи 286.

Несмотря на то, что в данном документе отсутствует специальная терминология, приведенная классификация киберпреступлений достаточно полно отражает сущность киберугроз.

Анализ структуры государственного аппарата КНР по обеспечению кибербезопасности представлен в работе Разумова Е.А. Особое место в обеспечении кибербезопасности принадлежит Военному совету ЦК КПК и Военному совету при Госсовете КНР. Структуру Госсовета КНР составляют: профильные министерства, в частности Министерство индустрии и информационных технологий, Министерство науки и технологий КНР, Министерство государственной безопасности, в частности одиннадцатое бюро министерства государственной безопасности КНР, отвечающее за радиоэлектронную разведку и компьютерную безопасность; ведущие малые группы, специализирующиеся на важных стратегических вопросах, в частности Центральная малая рабочая группа по внешней политике, Ведущая малая группа по вопросам национальной безопасности и Ведущая малая группа по проблемам Тайваня[[106]](#footnote-106).

Отдельно стоит осветить вопросы места и роли Народно-освободительной армии Китая (НОАК) в структуре обеспечения кибербезопасности КНР, которые были рассмотрены в работе Ибрагимовой Г. В структуре военного аппарата КНР стоит выделить третий департамент[[107]](#footnote-107). В его полномочия входит: разведывательная деятельность; поиск уязвимостей информационных сетей; разработка сценариев и проработка действий кибервойск по проведению кибератак на объекты цифровой инфраструктуры противника. Согласно отчету американских экспертов[[108]](#footnote-108), численность кибервойск КНР составляет 30 тысяч человек. В докладе также отмечается, что Китай регулярно проводит кибератаки на объекты США, преимущественно в разведывательных целях. Кроме того, в некоторых СМИ была опубликована информация о причастности военных хакеров из Китая к кибератакам на другие страны, в частности в 2019 году, были похищены данные японских IT компаний[[109]](#footnote-109).

На основании анализа политики обеспечения кибербезопасности КНР можно сделать вывод, что киберпространство в Китае рассматривается как специфическая информационная среда, которая подвержена значительной автономии, и в рамках которой происходит формирование современного Китая. При этом правительство КНР не только контролирует киберпространство страны, но и поддерживает и задает вектор развития информационных технологий, а также использует киберпространство для информационного воздействия и контроля населения Китая. Отличительной чертой китайского интернета является регламентация поведения пользователей в сети, пользователи имеют целый ряд обязанностей и ограничений, связанных с использованием интернета. Таким образом, кибербезопасность в Китае обеспечивается весьма жесткими, но эффективными и во многом беспрецедентными мерами, при этом рассмотренные киберугрозы в нормативно правовых актах КНР, во многом связаны с противодействием информационному воздействию иностранных государств и обеспечению безопасности и работоспособности критической информационной инфраструктуры. Очевидно, что киберпространству на текущем этапе развития КНР отведена особая роль в укреплении международного положения Китая. Киберпространство активно используется НОАК для проведения кибератак на объекты цифровой инфраструктуры противника, прежде всего с целью нанесения ущерба или сбора разведданных. Также НОАК взаимодействует с коммерческими и образовательными организациями, что обеспечивает доступ НОАК к передовым информационным исследованиям и технологиям, в том числе к средствам военного назначения. Стоит отметить, что кибервойска КНР на данный момент объективно могут считаться одними из наиболее боеспособных в мире и представляют опасность не только для прямых военных противников Китая, но и для политических и экономических соперников, а также технологических компаний и организаций, в частности российских.

# **2.3 Государственные стратегии кибербезопасности государств Евросоюза об основных угрозах в киберпространстве**

В отношении противодействия киберугрозам среди стран Европейского Союза (далее ЕС) можно выделить ряд государств, добившихся в этой области значительных успехов: Австрия, Франция, Норвегия, ФРГ, Швеция[[110]](#footnote-110). Учитывая транснациональный характер киберпреступности с одной стороны, и высокую степень взаимозависимости стран ЕС с другой[[111]](#footnote-111), компетентные органы государств-членов ЕС придерживаются единых стандартов при проведении политики кибербезопасности[[112]](#footnote-112). Стоит осветить основные документы и стандарты ЕС в сфере кибербезопасности.

В 2001 г. была подписана Конвенция Совета Европы «О киберпреступности», которая и по сей день является одним из основных документов, регулирующих правоотношения в сфере глобальной информационной сети по предотвращению и контролю преступности, связанной с применением компьютеров. В Конвенции[[113]](#footnote-113) имеются определения киберпреступлений, освещаются вопросы взаимодействия стран-членов Совета Европы в области обеспечения кибербезопасности. В 2004 г. образовано Европейское агентство по сетевой и информационной безопасности (ENISA), координирующее деятельность стран союза для борьбы с киберугрозами[[114]](#footnote-114). Стратегия кибербезопасности ЕС, принятая в 2013 году, содержит следующие положения[[115]](#footnote-115):

1. Стратегия предлагает расширение сотрудничества между государственными органами и частным сектором для противодействия трансграничным киберугрозам и координированию действий в чрезвычайных ситуациях.

2. Стратегия призывает государства-члены ратифицировать Будапештскую конвенцию Совета Европы о киберпреступности, и как можно скорее осуществить ее положения.

3. В целях повышения устойчивости кибербезопасности информационных систем, в области обороны и национальной безопасности, предлагается, развитие потенциала кибербезопасности в области обнаружения, реагирования и противодействия киберугрозам.

4. Разработка основ политики ЕС в области кибербезопасности, в частности проработка учебных курсов по кибербезопасности и координация деятельности между международными партнерами, включая НАТО.

Также, в 2013 году для усиления противодействия киберпреступности в ЕС учрежден Европейский центр киберпреступности, основные направления деятельности которого[[116]](#footnote-116):

1. Центр служит центральным узлом информации и разведки;

2. Центр поддерживает операции и расследования со стороны государств-членов, предлагая оперативный анализ, координацию и значительный опыт;

3. Центр предоставляет различные продукты стратегического анализа, которые позволяют принимать обоснованные решения на тактическом и стратегическом уровнях по борьбе с киберпреступностью и ее предупреждению;

4. Центр обеспечивает комплексную информационно-пропагандистскую функцию, связывающую правоохранительные органы, занимающиеся борьбой с киберпреступностью, с частным сектором, научными кругами и другими партнерами, не связанными с правоохранительными органами;

5. Центр поддерживает обучение и наращивание потенциала, в частности, для соответствующих органов в государствах-членах;

6. Центр предоставляет узкоспециализированные возможности технической и цифровой судебной поддержки расследованиям и операциям;

7. Центр представляет правоохранительное сообщество ЕС в областях, представляющих общий интерес (требования к исследованиям и разработкам, управление интернетом и разработка политики).

В 2016 году была согласована директива Европейского Союза «о безопасности сетевых и информационных сетей»[[117]](#footnote-117), согласно которой государства-участники, должны гарантировать наличия национальных систем кибербезопасности, включающих:

1. Стратегии в области информационной безопасности, а также соответствующую политику и регулятивные меры, направленные на поддержание высокого уровня безопасности сетей и информационных систем;

2. Национальные уполномоченные органы для мониторинга реализации директивы на территории определенного государства и помощи по ее последовательной реализации;

3. Единого канала взаимодействия по вопросу безопасности сетей и информационных систем между государствами-участниками, группой взаимодействия и сетью групп реагирования на инциденты, связанные с компьютерной безопасностью;

4. Одной или нескольких групп, отвечающих за управление рисками и инцидентами.

Также, в ЕС принят общий регламент защиты персональных данных (GDPR) – генеральный регламент о защите персональных данных, принятый для унификации и усилении персональных данных граждан государств ЕС[[118]](#footnote-118). GDPR является документом, состоящем из 99 статей, в которых подробно рассматриваются различные аспекты защиты персональных данных. Регламент существует в качестве основы для национальных стратегий государств ЕС.

ЕС активно сотрудничает с НАТО, так с 2008 г. в Эстонии функционирует Центр передового опыта НАТО по киберобороне – Международная военная организация, которая сосредоточивает свои усилия на расширении возможностей кибернетической обороны НАТО и стран-партнеров. НАТО официально признало киберпространство операционной средой и таким образом приравняло существующие в нем угрозы к военным угрозам. А, В 2017 г. в Таллинне был создан Объединенный центр передовых технологий по киберобороне НАТО. Центр получил аккредитацию НАТО, насчитывает 20 участников – 17 членов НАТО и три государства-партнера. Основная задача Центра – тренировка специалистов из разных стран, обеспечивающих безопасность в национальном киберпространстве[[119]](#footnote-119).

 Стоит отметить, что ввиду различия социального, технического и экономического уровня развития, не все страны ЕС способны в полной мере обеспечить соответствие национальных киберстратегий директивам и рекомендациям ЕС[[120]](#footnote-120).

Стратегия кибербезопасности Германии принята в 2011 г., основное внимание в Стратегии ФРГ уделено предотвращению кибератак, уголовному преследованию киберпреступлений, а также предупреждению выхода из строя физической составляющей информационных систем[[121]](#footnote-121). Согласно стратегии ФРГ, кибербезопасность - это желаемое состояние кибербезопасности, при которой риски исходящие из киберпространства сведены к приемлемому минимуму[[122]](#footnote-122).

Кибербезопасность в ФРГ разделяется на гражданскую и военную, где первая фокусируется на всех ИТ системах для гражданского использования в киберпространстве ФРГ, а вторая фокусируется на всех ИТ системах для военного использования в немецком киберпространстве. Несмотря на разделение кибербезопасности на военную и гражданскую в документе приведены лишь основные угрозы и вызовы, исходящие из киберпространства, без разделения на военные и гражданские, это[[123]](#footnote-123):

1. Атаки на критическую информационную инфраструктуру;

2. Кибертерроризм;

3. Кибершпионаж;

4. Использование киберпространства в военных целях;

5. Уязвимости новых информационных технологий;

6. Атаки на промышленные инфраструктуры, не относящиеся к критическим.

Также, в стратегии кибербезопасности ФРГ подчеркивается важность поддержания государством стабильности и доступности киберпространства для граждан Германии, в особенности для экономического сектора, при этом препятствие использованию киберпространства, признается недопустимым[[124]](#footnote-124). В разделе, регламентирующем уголовное наказание лиц, совершающих преступления в киберпространстве, указано, что транснациональный характер киберпреступности, требует тесного сотрудничества между правоохранительными органами разных стран, а также соблюдения международных норм, правил и стандартов[[125]](#footnote-125). В 2016 г. парламентом ФРГ был принят закон о кибербезопасности, дополняющий, изданную ранее стратегию кибербезопасности. Закон затрагивает вопросы обеспечения безопасности критической информационной инфраструктуры, в частности, согласно закону, поставщики информационных услуг обязаны в течение двух лет внедрить новые стандарты безопасности в киберпространстве. Рассматривается возможность внедрения в критические информационные инфраструктуры новых технологий кибербезопасности, в частности новые стандарты шифрования и идентификации пользователей[[126]](#footnote-126). В 2016-2017 в Германии было создано командование кибер и информационного пространства, представляющее собой отдельной компонент Бундесвера. Отличительной особенностью немецкого киберкомандования является его широкий функционал, помимо проведения киберопераций, оно занимается защитой информации и обеспечением кибербезопасности, радиоэлектронной борьбой, картографией, разведкой, и связью[[127]](#footnote-127).

В целом, подход Германии в обеспечении кибербезопасности нельзя назвать «стандартным» в сравнении с остальными странами ЕС, в которых основное внимание уделяется минимизации экономических потерь, связанных с киберугрозами. Подход Германии основан на разделении военной и гражданской кибербезопасности, являясь тем самым своего рода сбалансированным подходом.

Национальная стратегия кибербезопасности Австрии использует более широкую концепцию безопасности ИКТ и рассматривает кибербезопасность как защиту систем ИКТ с помощью конституционных средств от связанных с субъектом, технических, организационных и естественных опасностей, представляющих риск для безопасности киберпространства, включая инфраструктуру и безопасность данных, а также безопасность пользователей в киберпространстве[[128]](#footnote-128). Стратегия безопасности ИКТ является инициативной концепцией, направленной на защиту киберпространства и людей в этом виртуальном пространстве с учётом их основных прав и свобод. Конкретный подход страны к кибербезопасности тесно связан с существующими в ней наиболее заинтересованными сторонами и структурами – различными организациями, учреждениями или отдельными лицам[[129]](#footnote-129).

В сравнении с рассмотренными ранее стратегиями кибербезопасности, в Австрийской стратегии приведена одна из наиболее полных классификаций киберугроз. Согласно матрице кибер-рисков, представленной в приложении к стратегии[[130]](#footnote-130), киберугрозы условно можно разделить на 4 группы: маловероятные и неопасные; маловероятные и опасные; вероятные и неопасные; вероятные и опасные. Стоит отметить, что в стратегии кибербезопасности Австрии каждая киберугроза занимает свое определенное место в матрице рисков, по принципу системы координат, где ось Х - вероятности возникновения киберугрозы, а ось Y – потенциальный ущерб от угрозы. В приведенном далее перечне, киберугрозы рассматриваются от наименее вероятных к наиболее вероятным.

К маловероятным и неопасным относится манипуляция сигналом времени GPS[[131]](#footnote-131), поскольку, с одной стороны на гражданском уровне данная киберугроза с большой долей вероятности не повлечет фатальных последствий, а с другой стороны, на уровне критической информационной инфраструктуры, данные системы дублируются.

Маловероятные и опасные киберугрозы: технический сбой или взлом системы цифровой подписи; использование данных персональной идентификации граждан, распределенные атаки типа «отказ в обслуживании»; неправомерный доступ к системе контроля водоснабжения; неправомерный доступ к системе контроля подачи электроэнергии и поставки IT – услуг; непрофессиональные и халатные действия сотрудников критической информационной инфраструктуры; получение неправомерного доступа к спутниковой и цифровой связи; получение неправомерного доступа к финансовым операциям; захват контроля над критической информационной инфраструктурой. Наиболее вероятными источниками данного типа киберугроз, являются: техногенные катастрофы, естественные уязвимости информационных инфраструктур (например, человеческий фактор), кибертерроризм[[132]](#footnote-132) и кибервойна[[133]](#footnote-133).

Вероятные и неопасные киберугрозы: систематическое воровство персональных данных, социальная инженерия, отсутствие или устаревание правовой основы регулирования киберпреступлений, неосведомленность граждан о стандартах безопасности, отсутствие или неполное управление непрерывностью бизнеса, манипуляция и шантаж граждан через социальные сети, отсутствие аудита безопасности, неверное понимание статуса кибератаки[[134]](#footnote-134). Наиболее вероятными источниками данного типа киберугроз, являются: киберпреступность[[135]](#footnote-135) и технические дефекты или уязвимости IT систем.

Вероятные и опасные киберугрозы: неправомерный доступ к промышленным автоматическим системам управления, неправомерный доступ к облачным хранилищам данных, неправомерный физический доступ к IT системам при их транспортировке, недостаточность финансирования сферы кибербезопасности, отсутствие специалистов кибербезопасности, отсутствие или неясность ответственности учреждений использующих системы ИКТ, вредоносные программы или низкокачественные IT продукты, кибершпионаж[[136]](#footnote-136), неизвестные IT угрозы. Наиболее вероятными источниками данного типа киберугроз, являются: киберпреступность, кибертерроризм и кибервойна.

Таким образом, политика кибербезопасности Австрии предполагает тождественность категорий информационная безопасность и кибербезопасность и уделяет значительное внимание киберугрозам, создающим риски для экономического, стоит сказать, что такой подход характерен для большинства стран ЕС. При этом, в стратегии кибербезопасности Австрии представлена одна из наиболее подробных классификаций киберугроз среди государств, рассмотренных в данной работе.

Ещё одной страной ЕС, занимающей лидирующие позиции в глобальном индексе кибербезопасности[[137]](#footnote-137), является Швеция. Высокий уровень кибербезопасности в Швеции во многом обусловлен высоким уровнем экономического и социального развития страны. В стратегии кибербезопасности Швеции, которая была принята в 2016 году, под кибербезопасностью понимается комплекс мер безопасности, направленных на сохранение конфиденциальности, достоверности и доступности информации[[138]](#footnote-138).

Киберугрозы в стратегии кибербезопасности Швеции, представлены в более общем виде, в сравнении с Австрийской стратегией. Условно, представленные киберугрозы можно разделить по следующим категориям:

Угрозы, связанные с персональными данными и информацией: кибератаки в ходе, которых похищаются важные данные с целью дальнейшего использования или продажи; шантаж граждан при незаконном получении персональной информации; кража данных составляющих государственную или коммерческую тайну.

Угрозы, связанные с критической информационной инфраструктурой: нарушение функционирования системы управления страной в критических ситуациях; получение доступа или нарушение деятельности цифровых систем информации и контроля, которые постоянно обрабатывают большое количество конфиденциальной информации в целях контроля, например: распределение электроэнергии, водоснабжения, транспорта, транспортной инфраструктуры или больничного оборудования; атаки на промышленные объекты, использующие IT системы; инциденты и атаки, касающиеся шведской торговли и промышленности.

Киберугрозы, преследующие политические цели: кибершпионаж; кибератаки со стороны враждебных государств и спонсируемых ими субъектов; диверсии против критически важных объектов информационной инфраструктуры; неправомерный доступ к независимым средствам массовой информации и информационным агентствам; дезинформация через киберпространство.

В целом, структура стратегии кибербезопасности Швеции схожа, с рассмотренными ранее стратегиями государств ЕС, однако, отличительной чертой шведской стратегии, является более подробное рассмотрение киберугроз, связанных с защитой суверенитета Швеции от внешнего посягательства.

Подводя итог, стоит сказать, что стратегии кибербезопасности стран ЕС, в значительной мере отличаются от стратегий США и КНР. Учитывая взаимосвязь между состоянием кибербезопасности страны и уровнем экономического развития, киберпространство для европейских государств представляется инструментом достижения определенных экономических целей. Киберугрозы, упоминаемые в стратегиях, представлены в основном, в виде различных вариантов кибератак и в виде иных возможностей неправомерного использования киберпространства, что говорит о практической направленности стратегий кибербезопасности. Вопросы использования киберпространства для достижения глобальных геополитических или военных целей, в национальных стратегиях как правило не освещаются, за исключением стратегии Германии, однако этот вопрос регламентируется на наднациональном уровне. Государства-члены ЕС активно сотрудничают с НАТО в области обеспечения кибербезопасности, кроме того проводят совместные учения, направленные не только на предупреждение киберугроз, но и на проработку наступательных действий в киберпространстве, что безусловно создает дополнительное угрозы для Российской Федерации. Еще одним характерным моментом является тождественность категорий информационная безопасность и кибербезопасность.

# **Глава 3. КИБЕРОПАСНОСТИ И КИБЕРУГРОЗЫ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА В СОВРЕМЕННОЙ РОССИИ**

# **3.1 Роль информационной безопасности в обеспечении суверенитета Российской Федерации**

Современный этап развития человечества связан с процессами глобализации, которые характеризуются расширением сфер и увеличением масштабов применения информационных технологий. В политике Российской Федерации, информационным технологиям, в частности сети Интернет, также принадлежит значительная роль.

Под информационной безопасностью Российской Федерации понимают состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства[[139]](#footnote-139). Главной задачей государства в области информационной безопасности является обеспечение: суверенитета страны; конкурентоспособности отечественных информационных технологий; гарантий конституционных прав и свобод гражданина; безопасности критической информационной инфраструктуры [[140]](#footnote-140).

 Согласно доктрине информационной безопасности Российской Федерации, информационная сфера представляет собой совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет", сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений[[141]](#footnote-141).

В структуре политики информационной безопасности целесообразно выделить два основных направления — государственно-правовое и технологическое. Государственно-правовое направление политики обеспечения информационной безопасности связано с функционированием органов исполнительной и законодательной власти и с состоянием законодательной и нормативно-правовой базы[[142]](#footnote-142). В Доктрине информационной безопасности Российской Федерации[[143]](#footnote-143) сформулированы основные принципы, направления и задачи государственной политики обеспечения информационной безопасности Российской Федерации. Согласно доктрине, система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности[[144]](#footnote-144).

Интернет на сегодняшний момент является одной из главнейшей составляющей информационной сферы России. Аудитория интернета в Российской Федерации ежегодно увеличивается. По данным исследования[[145]](#footnote-145) компании Mediascope, на настоящий момент, интернетом пользуется 95,8 миллионов человек, что составляет 78 % населения страны. Объем рынка Интернет-торговли в настоящий момент превышает 1,66 трлн. рублей [[146]](#footnote-146), что на 59 % выше, чем данный показатель в предыдущем году, таким образом, данный сектор экономики является самым эффективным по темпам роста, и, согласно прогнозам[[147]](#footnote-147), к 2022 году, составит 3 трлн. рублей. Сегодня интернет – независимая и доступная система коммуникации, включающая в себя такие средства представления и пересылки информации, как электронная почта, веб-сайты, различные протоколы передачи данных, что делает интернет не только фактором экономического роста и развития, но и фактором формирования международных отношений[[148]](#footnote-148).

Также, чтобы определить роль информационной безопасности в обеспечении суверенитета России, необходимо рассмотреть наиболее разрушительные по своему воздействию угрозы информационной безопасности Российской Федерации, представленные в доктрине информационной безопасности[[149]](#footnote-149), это: наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях; расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия; использование механизмов информационного воздействия на индивидуальное, групповое и общественное сознание террористическими и экстремистскими организациями; возрастание масштабов компьютерной преступности; недостаточный уровень развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг.

**Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.**

В 2009 году глава агентство национальной безопасности США заявил о начале формирования кибервойск, как специального подразделения Стратегического командования США[[150]](#footnote-150). Согласно данным исследования Zecurion Analytics, численность кибервойск США, составляет 9 тысяч человек, при финансировании около 7 млрд. долларов в год[[151]](#footnote-151). Численность ИТ-специалистов армии КНР, достигает 20 тысяч человек, финансирование которых обходится бюджету страны в 1,5 млрд. долларов в год[[152]](#footnote-152). В 2015 г. КНР принята военная стратегия, согласно которой необходимо мобилизовать систему национальной обороны с целью обеспечения адекватного реагирования на чрезвычайные ситуации и достижения победы в информационной войне[[153]](#footnote-153). Мощные, в сравнении с остальными странами, группировки кибервойск также присутствуют в Великобритании, Южной Корее и Российской Федерации, с численностью 2000, 700 и 1000 человек, и объемом финансирования 450, 400 и 300 млн. долларов соответственно[[154]](#footnote-154).

**Расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия.** В работе доктора политических наук Сулеймановой Ш.С. и доктора политических наук Назарова Е.А. «Информационные войны: история и современность» рассмотрены 5 теорий ведения современных информационных войн[[155]](#footnote-155).

Использование авторитетов - использовании авторитетных, известных для целевой аудитории людей или групп. Группами влияния являются: известные политические деятели, руководители предприятий, преподаватели учебных заведений, деятели культуры т.д. Эффективность данного метода, зависит от наличия следующих факторов: доверие к представителю группы влияния, известность представителя, наличие профессиональных качеств, личные достижения и достоинства, высокий официальный пост, близость с целевой группой электората[[156]](#footnote-156).

Имитационная дезинформация - внесение изменений в пропаганду другой стороны, придающих ей другое направление, снижающих доверие к ней, создающих негативный образ. Используется в виде подмены листовок, высказываний кандидатов или групп[[157]](#footnote-157).

Псевдологические выводы - использование неправильных логических выводов, с целью формирования «выгодной» повестки дня[[158]](#footnote-158).

Принуждающая пропаганда - данная теория информационного воздействия заключается в использовании слов и выражений, имеющие принуждающий характер[[159]](#footnote-159).

Наклеивание ярлыков - эксплуатация предрассудков и стереотипов населения через "навешивание ярлыка". Ярлык квалифицирует этот объект как что-то, чего аудитория боится, ненавидит, испытывает отвращение, находит подозрительным или нежелательным и др.

**Использование механизмов информационного воздействия на индивидуальное, групповое и общественное сознание террористическими и экстремистскими организациями.** Мкртчян А.А. в своей работе[[160]](#footnote-160) обозначил террористический акт как способ психологического воздействия, цель которого вызвать негативные психологические последствия, носящие долговременный характер. Среди таких последствий он выделил посттравматическое стрессовое расстройство, страх, панику, «Стокгольмский синдром», легитимизацию агрессии, которые назвал преобладающими[[161]](#footnote-161). Главной целью террористических акций автор обозначил аудиторию средств массовой информации. «При этом, влияние СМИ может быть, как положительным, так и отрицательным. Так, например, непрофессиональное освещение событий способствует искажению информации, которая усиливает отрицательное эмоциональное состояние людей, повышает степень страха и паники, способствует легитимизации насилия» [[162]](#footnote-162).

**Возрастание масштабов компьютерной преступности.** В соответствии с данными Прокуратуры РФ количество Интернет-преступлений в период с 2018 по 2019 год претерпело значительное увеличение — составив 180153 эпизод[[163]](#footnote-163). Их доля от числа всех зарегистрированных в России преступных деяний составляет примерно 12%. Самыми распространенными преступлениями в сети Интернет, являются неправомерный доступ к компьютерной информации создание, использование и распространение вредоносных компьютерных программ. Ущерб от киберпреступлений в 2019 году составил почти 2.5 трлн рублей. Это на 66% больше аналогичного показателя прошлого года. По оценкам экспертов, в 2020 году, этот показатель может достигнуть 3-4 трлн рублей, что составляет 17% от бюджета Российской Федерации 2020 года[[164]](#footnote-164).

Таким образом, роль информационной безопасности в обеспечении суверенитета Российской Федерации, обусловлена: возрастающей ролью информационных технологий и интернета в жизни Российского общества; увеличением аудитории сети-интернет; увеличением роли интернета, в экономике и государственном управлении; разрушительным характером ряда угроз информационной безопасности; значительными потерями российской экономики из-за киберпреступлений; вероятностью возникновения военных конфликтов в информационном пространстве.

# **3.2 Нормативные документы Российской Федерации по обеспечению информационной безопасности об опасностях и угрозах в киберпространстве**

Начиная с 2013 года, наметилась мировая тенденция смещения акцентов национальных стратегиях информационной безопасности. Если раньше приоритетом являлась защита граждан и организаций в киберпространстве, то сейчас стратегии нацелены прежде всего на защиту отдельных институтов и общества в целом[[165]](#footnote-165). В Российской Федерации в настоящий момент, можно выделить ряд нормативных документов, в которых обозначены актуальных кибреугрозы.

Тенденции, отмеченные в Военной доктрине Российской федерации[[166]](#footnote-166), указывают на смещение военных угроз и опасностей в информационное пространство и внутреннюю сферу Российской Федерации и повышение значимости информационных технологий в современных военных конфликтах. Среди угроз военных угроз и опасностей, указанных в доктрине, также можно выделить киберопасности и киберугрозы:

1.Использование информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности;

2.Деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющая целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества.

В концепции внешней политики Российской Федерации[[167]](#footnote-167) указано, что в современном мире для реализации геополитических интересов государства, наряду с военной мощью, используют информационные и технологические ресурсы. Применение инструментов «мягкой силы[[168]](#footnote-168)», путем использования информационно-коммуникационных технологий становится неотъемлемой частью современной мировой политики.

Документом, в котором наиболее полно отражены угрозы информационной безопасности и киберугрозы в частности, является доктрина информационной безопасности Российской Федерации[[169]](#footnote-169). Среди перечня угроз информационной безопасности, к киберугрозам могут быть отнесены следующие:

1.Использование информационно-коммуникационных технологий, в частности сети-интернет, для обмена информации в военно-политических, криминальных, террористических и экстремистских целях;

2.Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру Российской Федерации в военных целях;

3.Использование информационно-технических средств для разведывательных целей в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса;

4.Использование специальными службами иностранных государств средств информационно-психологического воздействия, направленного на дестабилизацию внутриполитической ситуации в различных регионах мира и России, в частности;

5.Кибератаки и иные виды компьютерных преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий;

6.Зависимость российской промышленности от зарубежных информационных технологий, недостаточный уровень развития конкурентоспособных отечественных информационных технологий

Наиболее резонансным законопроектом, по защите критической информационной инфраструктуры, стал Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон „О связи“ и Федеральный закон "об информации, информационных технологиях и о защите информации", более известный как «Закон о суверенном интернете». Возможность автономизации российского интернет пространства, активно обсуждалась после событий 2014 года, когда ввиду санкций, появилась вероятность отключения России от мировой сети[[170]](#footnote-170).

В соответствии с законопроектом российские интернет-провайдеры должны принять технические меры в своих сетях для противодействия потенциальным угрозам со стороны иностранных агрессоров - по сути, изолировать российский интернет от остальной части сети и обеспечить передачу всего трафика через внутренние системы страны[[171]](#footnote-171).

Финансовым инструментом, который активно используются для легализации доходов, полученных нелегальным путем, и для осуществления финансовых операций является криптовалюта[[172]](#footnote-172). Технические особенности ряда криптовалют, позволяют проводить анонимные денежные операции, чем активно пользуются преступные и террористические организации. В настоящее время, в Российской Федерацией, разработан законопроект № 419059-7 «О цифровых активах» [[173]](#footnote-173), направленный на регулирование отношений, возникающие при создании, выпуске, хранении и обращении цифровых финансовых активов, а также осуществлении прав и исполнении обязанностей по смарт-контрактам. Согласно законопроекту, Федеральная служба по финансовому мониторингу будет регулировать все операции с цифровыми валютами в Российской Федерации в соответствии с международной группой разработки финансовых мер по борьбе с отмыванием денег (FATF). Должностные лица будут регистрировать и проверять биржи и платформы ICO[[174]](#footnote-174). Кроме того, комиссия будет обязана проверять деятельность, связанную с традиционными активами, на сумму более 600 000 рублей[[175]](#footnote-175).

В Российской Федерации, в настоящее время отсутствует единый нормативный документ, регулирующий киберпространство. Таким документом может стать стратегия кибербезопасности Российской Федерации[[176]](#footnote-176), находящаяся в стадии разработки. Киберугрозы представлены в разрозненном виде, в различных нормативных документах, как правило посвященных различным составляющим национальной безопасности Российской Федерации. Характерной чертой киберугроз представленных в российских нормативных документах, является их милитаристическая направленность, из рассмотренных выше киберугроз, только две связаны с компьютерной преступностью.

# **3.3 Перспективы защиты России от иностранных информационных интервенций и кибервоздействий.**

В связи с высокими темпами информатизацией всех сфер жизни общества, включая и военную сферу, значительное внимание в научной среде уделяется исследованиям, по ведению информационного противоборства[[177]](#footnote-177); издаются правительственные документы и уставы вооруженных сил различных стран[[178]](#footnote-178). В.Е. Макаров в своей монографии указал, что операции информационно-психологического воздействия в информационном обществе являются основной формой экспансии, используемой государствами для распространения своего влияния на другие субъекты геополитической конкуренции, а также, в целях защиты национальных интересов и обеспечения государственной безопасности[[179]](#footnote-179).

В локальных война и военных конфликтах, в особенности к которым причастны формирования ВС США и объединённые вооруженные силы НАТО, активно прорабатываются, проверяются и используются технологии информационного воздействия. Большинство военных конфликтов[[180]](#footnote-180), двух последних десятилетий, начинались с мощного информационного воздействия. В качестве примера могут быть приведены конфликты в Югославии, Иране, Афганистане и др.

Макаренко С.И., в своей монографии, где в частности рассматривает различные модели информационного противоборства, пишет, что в 1995 г. компанией RAND Corporation был проведен ряд исследований с целью выявления национальных приоритетов в концепции информационного противоборства США. Результат этих работ был изложен в отчете MR-661-OSD. В дальнейшем полученные результаты получили свое эволюционное развитие в виде классификации поколений стратегического противоборства и были опубликованы в отчете MR-964-OSD[[181]](#footnote-181).

Стратегическое информационное противоборство первого поколения используется в качестве обеспечение действий традиционных сил и средств, и в большей степени ориентировано на дезорганизацию деятельности систем управления[[182]](#footnote-182).

Стратегическое информационное противоборство второго поколения представляет принципиально новый тип стратегического противоборства, который вводит в круг сфер противоборства информационное пространство и ряд других областей. Информационное противоборство второго типа может быть растянуто во времени на недели, месяцы и годы. Среди задач, которые решающихся посредством ведения информационного противоборства второго поколения, можно выделить наиболее разрушительные по своим последствиям[[183]](#footnote-183):

1. Манипулирование общественным сознанием с целью создания политической напряженности;

2. Дестабилизация отношений между политическими партиями, объединениями и движениями с целью провокации различных конфликтов;

3. Подрыв уровня информационного обеспечения органов власти и управления;

4. Подрыв авторитета и дискредитация государственных органов управления в глазах населения;

5. Провоцирование столкновений на социально, политической, национальной и религиозной почве;

6. Инициирование акций экономического протеста;

7. Воспрепятствование принятия органами управления важных решений;

8. Подрыв международного авторитета государства;

9. Нанесение ущерба стратегическим интересам государства в различных сферах.

В работе Паршина С. А., Горбачева Ю. Е. и Кожанова Ю. А. «Кибервойны — реальная угроза национальной безопасности» направления задач информационного воздействия представлены в более общем виде[[184]](#footnote-184):

1. Разведывательное направление, с целью получения информации о военном, экономическом, культурном и политическом потенциалах государства;

2. Уничтожение, искажение или подавление информации, вывод из строя систем информационной инфраструктуры;

3. Виртуальное отображение оперативной информации об обстановке в реальном времени (визуализация поля боя);

4. Создание информации, несоответствующей реальной информации, имеющей характер информационно-психического и физического воздействия на граждан.

Перспективы защиты Российской Федерации от иностранных информационных интервенций и кибервоздействий таким образом, напрямую связаны с противодействием различным задачам и направлениям информационного воздействия. Анализ системы обеспечения информационной безопасности Российской Федерации, позволяет сделать следующие выводы:

1. Проведенный анализ киберугроз в нормативных документах Российской Федерации свидетельствует о том, что в России в настоящее время отсутствует общее понимание совокупности киберугроз. Нет ясного и четкого представления о том, кто является действительным источником угроз информационной безопасности и киберугроз, в частности. И нет четкой регламентации противодействия этим угрозам.

2. Государственные органы и государственные компании Российской Федерации, используют информационные системы и программное обеспечение иностранного производства, которые могут быть использованы, например, в период санкций как механизм информационного орудия при конкурентной борьбе или в качестве инструмента кибершпионажа. Несмотря на то, что доля отечественного программного обеспечения увеличилась с 20% в 2015 году до 65% в 2020[[185]](#footnote-185), имеющиеся 35% иностранного программного обеспечения способны оказать значительное негативное влияние на работоспособность российских государственных органов и компаний в критической ситуации.

3. Зависимость экономики Российской Федерации от иностранных финансовых сервисов, которые могут быть использованы в качестве средства оказания негативного воздействия на состояние экономики Российской Федерации. Так, по состоянию на 2019 год, доля операций российских платежных систем на российском рынке составляет около 20% от общего числа произведенных операций[[186]](#footnote-186). Данная ситуация, может быть использована в целях оказания давления на российскую экономику иностранными государствами. К примеру, платежные системы VISA и MASTERCARD, регулярно блокируют карты российских компаний и банков, которые находятся под действием американских санкций[[187]](#footnote-187).

4. Наблюдается положительная тенденция динамики роста доли организаций, использующих средства защиты информации, передаваемой по глобальным сетям, в общем числе российских организаций. Согласно данным государственной программы Российской Федерации «Информационное общество» [[188]](#footnote-188) в 2020 году доля таких организаций составляет 90%, в сравнении с 70% в 2010 году.

5. Наблюдается тенденция повышении компьютерной грамотности среди российского населения. Об этом свидетельствует увеличение доли населения, которая использующих средства защиты информации, и на данный момент составляет более 83% от числа пользователей[[189]](#footnote-189).

6. Нельзя однозначно оценить степень защиты граждан Российской Федерации от информационно-психологического воздействия. С одной стороны, важность внимания к такому роду угроз подчеркнута во многих нормативных документах Российской Федерации[[190]](#footnote-190), а с другой стороны, мероприятия по противодействию данным угрозам в нормативных документах присутствуют в разрозненном виде.

7. Однозначно можно констатировать зависимость России от иностранных компьютерных комплектующих. В частности, доля отечественных микропроцессоров на российском рынке крайне мала из-за их низкой производительности, в сравнении с зарубежными образцами[[191]](#footnote-191).

8. Согласно отчету всемирной организации интеллектуальной собственности за 2019 год[[192]](#footnote-192), по количеству патентных заявок в целом, и в области компьютерных технологий в частности, Российская Федерация занимает 8 место. При этом количество патентных заявок Китая, занимающего 1 место в данном рейтинге, больше количества российских заявок в 32 раза.

Сопоставление рассмотренных потенциальных задач, решающихся в рамках информационного воздействия и анализа текущего состояния информационной безопасности Российской Федерации, позволяет сделать вывод что несмотря на положительную тенденцию увеличения доли компаний и граждан, использующих средства защиты информации, внедрения российского программного обеспечения и создания российской платежной системы, нельзя сказать, что информационное воздействие на Российскую Федерацию полностью невозможно. Прежде всего, все еще имеющаяся зависимость от иностранных компьютерных технологий и программного обеспечения создает угрозу утечки данных и кибершпионажа, остается возможность информационно-психологического воздействия на граждан России, существует опасность технического отставания Российской Федерации в информационно-технической сфере, сохраняющаяся зависимость от иностранных финансовых сервисов создает возможность экономического давления на Россию.

**ЗАКЛЮЧЕНИЕ**

Процессы информатизации, происходящие в мире закономерно, расширяют направления использования информационных технологий, которые на сегодняшний момент проникли практически во все сферы жизни общества, что в свою очередь приводит к появлению новых угроз безопасности государств. Сложившаяся ситуация приводит к повышению значимости кибербезопасности в системе глобальной и национальной безопасности, как следствие вопрос противодействия киберугрозам и киберопасностям в настоящее время является актуальной проблемой. Вместе с тем, в научной среде нет единого определения терминов «киберпространство», «кибербезопасность», «киберопасность» и «киберугроза», также, в различных нормативных документах некоторых развитых стран, в частности в национальных киберстратегиях, кибербезопасность рассматривается как тождественное информационной безопасности.

В Российской Федерации процессы диверсификации цифровой инфраструктуры, приводят к проникновению информационных технологий в различные сферы жизни российского общества. Проведённый анализ процесса диверсификации информационной инфраструктуры позволяет сделать вывод, что, данный процесс приводит к расширению перечня киберугроз. Такие факторы как: возрастающая роль информационных технологий и интернета в жизни Российского общества; увеличение аудитории сети-интернет; увеличение роли интернета, в экономике и государственном управлении; разрушительный характер ряда угроз информационной безопасности; возможность возникновения военных конфликтов в информационном пространстве приводят к увеличению значимости информационной безопасности в обеспечении суверенитета Российской Федерации. Также стоит выделить ряд проблемных моментов обеспечения информационной безопасности и кибербезопасности Российской Федерации: национальная киберстратегия России существует исключительно в форме проекта; сохраняется зависимость Российской Федерации от иностранных информационных продуктов и сервисов; значительная доля иностранного программного обеспечения, используемая в органах государственной власти, создает угрозы для утечек информации.

Политика США в области киберпространства и кибербезопасности, в первую очередь направлена на достижение информационного превосходства, наряду с задачами обеспечения безопасности киберпространства, в рассмотренных нормативных документах обозначены политические цели, которые достигаются в частности путем проведения кибератак на виртуальное пространство противника, которые осуществляют специализированные военные подразделения.

Политика обеспечения кибербезопасности КНР прежде всего предполагает значительную автономию китайского киберпространства. Правительство КНР контролирует киберпространство страны, поддерживает развитие информационных технологий, а также использует информационные технологии для информационного воздействия и контроля населения Китая. Китайский интернет предполагает значительную регламентацию поведения пользователей в сети и полностью устраняет анонимность в сети. НОАК также активно использует киберпространство для проведения кибератак на объекты цифровой инфраструктуры противника, прежде всего с целью нанесения ущерба или сбора разведданных.

Характерной чертой политики кибербезопасности государств-членов ЕС, является тождественность категорий информационная безопасность и кибербезопасность. Учитывая взаимосвязь между состоянием кибербезопасности страны и уровнем экономического развития, киберпространство для европейских государств представляется инструментом достижения определенных экономических целей. Киберугрозы, упоминаемые в стратегиях, представлены в основном, в виде различных вариантов кибератак и в виде иных возможностей неправомерного использования киберпространства, что говорит о практической направленности стратегий кибербезопасности. Вопросы использования киберпространства для достижения глобальных геополитических или военных целей, в национальных стратегиях как правило не освещаются, за исключением стратегии Германии, однако этот вопрос регламентируется на наднациональном уровне. Государства-члены ЕС активно сотрудничают с НАТО в области обеспечения кибербезопасности, кроме того проводят совместные учения, направленные не только на предупреждение киберугроз, но и на проработку наступательных действий в киберпространстве.

#

# **СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ**

**Нормативные акты**

1. Резолюция ГА ООН A/RES/56/19 от 29 ноября 2001 г. // ГЕНЕРАЛЬНАЯ АССАМБЛЕЯ ООН - Режим доступа: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf (дата обращения: 24.03.2019).
2. Резолюция ГА ООН 73/27 от 5 декабря 2018 [Электронный ресурс] // ГЕНЕРАЛЬНАЯ АССАМБЛЕЯ ООН - Режим доступа: https://undocs.org/ru/A/RES/73/27 (дата обращения: 24.03.2019).
3. Резолюция ГА ООН 73/266 от 22 декабря 2018 [Электронный ресурс] // ГЕНЕРАЛЬНАЯ АССАМБЛЕЯ ООН - Режим доступа: https://www.un.org/en/ga/search/view\_doc.asp?symbol=A/RES/73/266&Lang=R (дата обращения: 24.03.2019).
4. ISO/IEC 27032:2012. Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности. 2012.
5. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // ФГБУ «Редакция «Российской газеты», 1998-2020. – Режим доступа: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>. (дата обращения: 17.03.2020). – Загл. с экрана.
6. Концепция внешней политики Российской Федерации (утв. Президентом РФ 30.11.2016). [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_172989/bc3ab3b04947fc07f452721c58aacccf873d06b6/ (дата обращения: 21.03.2020).
7. Концепция стратегии кибербезопасности российской федерации (проект) [Электронный ресурс] // Совет Федерации Федерального Собрания Российской Федерации. – Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf. (дата обращения: 22.03.2020). – Загл. с экрана.
8. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ; Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 28.04.2015 г.) // СПС Консультант плюс.
9. Федеральный закон (проект) № 419059-7 "О цифровых финансовых активах" [Электронный ресурс] // Инфо-Бухгалтер. – Режим доступа: https://www.ib.ru/law/81/ (дата обращения: 24.03.2020).
10. Федеральный закон от 01.05.2019 N 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации" [Электронный ресурс] // Консультант плюс. – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_323815/ (дата обращения: 24.03.2019).
11. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"
12. Федеральный закон от 3 апреля 2005 года N 149 " Об информации, информационных технологиях и о защите информации " [Электронный ресурс] // Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения: 17.04.202020).
13. A national cyber security strategy (2016) [Электронный ресурс] // Government offices of Sweden – Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy (дата обращения: 07.03.2020).
14. Austrian Cyber Security Strategy (2013) [Электронный ресурс – Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy (дата обращения: 07.03.2020).
15. Clinton William. National Security Strategy / Washington DC: Government Printing Office. February 1995. P. 8.
16. Convention on Cybercrime, Budapest, 2001 [Электронный ресурс] // Official web-site of Council of Europe. Режим доступа: http:// conventions.coe.int./Treaty/en/Treaties/Html/185.htm (дата обращения: 17.05.2020).
17. Cyber Security Strategy for Germany (2011) [Электронный ресурс] // Federal Ministry of the Interior – Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany (дата обращения: 05.03.2020).
18. Cyber Strategy 2018 [Электронный ресурс] / Department of Defense Summary – 2018 - Режим доступа: https://media.defense.gov/2018/ Sep/18/2002041658/-1/-1/1/CYBER\_STRATEGY\_SUMMARY\_FINAL.PDF (дата обращения: 01.10.2018).
19. Cybersecurity and Infrastructure Security Agency Act of 2018 [Электронный ресурс] // The White House. – Режим доступа: https://www.congress.gov/bill/115th-congress/house-bill/3359 (дата обращения: 15.05.2020).
20. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [Электронный ресурс] // Brussels, 7.2.2013 JOIN (2013) 1 final Режим доступа: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec\_comm\_en.pdf (дата обращения: 17.05.2020).
21. Declaration by the Committee of Ministers on Internet Governance Principles, 2011 // https://wcd.coe. int/ViewDoc.jsp?id=1835773
22. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [Электронный ресурс] // Official Journal of the European Union. Режим доступа: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L\_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата обращения: 17.05.2020).
23. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. // U.S. Department of Homeland Security. 17.12.2003. Режим доступа: https://www.dhs.gov/homeland-security-presidential-directive-7 (дата обращения: 25.02.2020).
24. Information Warfare: Department of Defense Directive. TS 3600.1. December 21, 1992 [Электронный ресурс]. – Режим доступа: http://www.dod.mil/pubs/foi/administration\_and\_Management/admin\_matters/14F0492\_doc\_01\_Directive\_TS-3600-1.pdf (дата обращения: 29.03.2020).
25. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [Электронный ресурс] // Official Journal of the European Union.: http://data.europa.eu/eli/reg/2016/679/oj (дата обращения: 17.05.2020).
26. The Comprehensive National Cybersecurity Initiative [Электронный ресурс] // The White House. – 2008- Режим доступа: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurityinitiative (дата обращения: 15.05.2020).
27. The National Strategy to Secure Cyber Space / The White House, Washington DC, USA, 2003 // The White House. 2003. Режим доступа: http://georgewbush-whitehouse.archives.gov/pcipb/ (дата обращения: 25.02.2018).
28. U.S. Cyber Command’s Malware Inoculation: Linking Offense and Defense in Cyberspace [Электронный ресурс] // Council of foreign relation. – Режим доступа https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace. (дата обращения: 23.03.2020).

**Книги и периодические печатные издания**

1. Анализ текущего состояния развития цифровой экономики в России. М.: Институт развития информационного общества, 2018. — С. 50.
2. Атаманов Г.А. Информационная безопасность: сущность и содержание / Г.А. Атаманов // Бизнес и безопасность в России. - 2007. - N 47. - С. 108.
3. Безкоровайный М.М. Кибербезопасность подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. - 2014. - №1 (2) - С. 22-27.
4. Бухарин С. Н. Методы и технологии информационных войн / С. Н. Бухарин, В. В. Цыганов — М.: Академический проект, 2007. — 382 с.
5. Войскунский А.Е. Метафоры интернета / А.Е. Войкунский // Вопросы философии. 2001. № 11. С. 64–79.
6. Гриняев С. Н. Поле битвы — киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев — М.: Харвест, 2004. — С. 198-199.
7. Гуцев М.В. Диверсификация на высокотехнологичных предприятиях / М.В. Гуцев // Журнал Актуальные проблемы гуманитарных и естественных наук. – 2019. – №10/2011 – С.13.
8. Дзялошинский, И. М. Информационное пространство России: структура, особенности функционирования, перспективы эволюции / И. М. Дзялошинский. – Моск. центр Карнеги, М.: – 2001. – 30 с
9. Душкин Р. В. Обзор текущего состояния квантовых технологий. / Р.В. Душкин // Компьютерные исследования и моделирование – 2018. - Т. 10 - № 2 - С. 165
10. Жаворонкова Т.В Использование сети интернет террористическими и экстремистскими организациями / Т.В. Жаворонкова // Вестник Оренбургского государственного университета – 2015. – № 3 – С. 35.
11. Жаглин А. В. Понятийный аппарат теории национальной безопасности/ А.В Жаглин // Вестник Воронежского института МВД России – 2014. – № 3 – С. 160.
12. Запечников С.В. Проблемы обеспечения информационной безопасности больших данных / С. В. Запечников, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой // Безопасность информационных технологий. - 2014. - Т. 21. - №. 3. - С. 9
13. Зубарев И.В. Кибербезопасность автоматизированных систем управления военного назначения / И.В. Зубарев, И.В. Жидков, И.В. Кадушкин // Вопросы кибербезопасности. - 2013. - № 1(1). - 12 с.
14. Ибрагимова Г. Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечение информационной безопасности // Индекс безопасности. 2013. № 1 (104). С.169—184.
15. Ирошников Д. В. Соотношение понятий "опасность", "угроза", "вызов" и "риск" в правовой доктрине, действующем законодательстве и документах стратегического планирования/ Д.В. Ирошников // Транспорт, право и безопасность – 2017. – № 12 – С. 97.
16. Калашников А.О. новых технологий на информационную безопасность критической информационной инфраструктуры/ А.О. Калашников, Е.В. Аникина // Информация и безопасность – 2019. – № 2 – С. 56.
17. Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности / А.Я. Капустин // Журнал зарубежного законодательства и сравнительного правоведения – 2017. – № 6 – С. 48
18. Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни / Н.В. Кардава //Каспийский регион: политика, экономика, культура – 2019. – № 3(60). С. 74-76.
19. Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. д-ра юрид. Наук / М.Б. Касенова. -М., 2016 - С.27
20. Кедровский О.В. Информационное пространство России / О.В.Кедровский // Информационные ресурсы России. —1994. — № 4. — C. 2—3.
21. Лазарев И.А. Информация и безопасность. Композиционная технология. М.: Изд-во Московского городского центра научно-технической информации, 2002.
22. Лопатин В.Н. Информационная безопасность России: человек, общество, государство / В.Н. Лопатин // Серия: Безопасность человека и общества. СПб.: Фонд Университет, 2000. С. 428.
23. Лихтин А.А. Теоретические аспекты понятия «информационная политика» и особенности ее реализации в современной российской общественно-политической реальности /А.А. Лихтин, А.А. Ковалев// Управленческое консультирование. — 2017. — №1 (97). — С. 32
24. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: Монография / С.И. Макаренко — СПб.: Наукоемкие технологии, 2017. — с.225-227.
25. Макаров В.Е. Политические и социальные аспекты информационной безопасности: Монография / В.Е. Макаров. Таганрог. Изд. С.А. Ступин. 2006. – с.105.
26. Мкртычян А.А. Влияние средств массовой информации на психологические последствия терроризма: автореф. дис. канд. псих. наук. / А.А. Мкртычян – М.: Моск. гос. ун-т им. М.В. Ломоносова, 2012. – С. 37.
27. Мурзин Ф.А. Облачные технологии: основные понятия, задачи и тенденции развития / Ф.А. Мурзин, Т.В. Батура, Д.Ф Семич // Программные продукты, системы и алгоритмы. - 2014. - № 1. - С. 64.
28. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений. — 4-е изд., М., 1997. — 944 с.
29. Паршин С. А. Кибервойны — реальная угроза национальной безопасности / С. А. Паршин, Ю. Е. Горбачев, Ю. А. Кожанов — М.: КРАСАНД, 2011. — 96 с
30. Потапов А.С. Технологии искусственного интеллекта / А.С. Потапов – СПб: СПбГУ ИТМО, 2010. С.3
31. Проценко Е.А. Модель и метод анализа эффективности систем защиты информации сайтов органов власти Российской Федерации: Автореф. дис. канд. технич. наук. / Е.А. Проценко - СПб., 2008.
32. Стрельцов А.А. Содержание понятия "обеспечение информационной безопасности" // Информационное общество. - 2001. - №. 4. - С. 16.
33. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017. с. 81-85.
34. Умерова И.А. Экономические связи между странами-членами ЕС как фактор регионального единства и развития: диссертация кандидата экономических наук / И.А. Разумова Российский университет дружбы народов, Москва, 2009.
35. Уфимцев Ю.С., Ерофеев Е.А. и др. Информационная безопасность России. М.: Экзамен, 2003.
36. Философский словарь / Под ред. И.Т. Фролова. — М.: Республика, 2001. — С. 356
37. Цветков В.Я. Кибер физические системы / В. Я. Цветков // Международный журнал прикладных и фундаментальных исследований. – 2017. – № 6-1. – С. 64
38. Чеботарева А.А., Научные подходы к определению понятия "информационная безопасность" / А.А. Чеботарева // Информационное право – 2011. - №1. С. 3-6.
39. Шелкоплясова Н.И. Роль войск информационных операций в защите интересов национальной безопасности / Н.И. Шелкоплясова // [Вестник тульского филиала финуниверситета](https://www.elibrary.ru/contents.asp?id=39560579). - 2019. - № 1. С. 125.
40. Шишкина Т.С. Преимущества и недостатки внедрения стратегии диверсификации / Т.С. Шишкина // Актуальные проблемы экономики современной России. - 2015. - № 2. - С. 339-348.
41. Янковская Ю. Ю. Стойкость квантовых протоколов распределения ключей / Ю.Ю. Янковская, А. А. Марина // Сomputer sciences and telecommunications — 2013. — C. 2

**Зарубежная литература**

1. Kerschischnig G. Cyberthreats and International Law. / G. Kerschischnig - The Hague, 2012. - P. 5.
2. Ploug T. Ethic sin cyberspace: how cyberspace may influence interpersonal interaction. Dordrecht, 2009. P. 69–70.
3. Ventre D. Chinese Cybersecurity and Defense. London, Wiley­ISTE Publ., 2014, 301 p.
4. Wellman B. Physical place and cyberplace: the rise of personalized networking // International Journal of Urban and Regional Research. 2001. Vol. 25 (2). P. 247.

**Электронные ресурсы**

1. EUROPEAN CYBERCRIME CENTRE - EC3 [Электронный ресурс] // Europol Режим доступа: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (дата обращения: 17.05.2020).
2. Global Cybersecurity Index (GCI) (2018) [Электронный ресурс] // International Telecommunication Union – Режим доступа: https://www.itu.int/dms\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (дата обращения: 05.03.2020).
3. Khalimonenko, А. DDOS attacks in Q1 2017 [Электронный ресурс] /А. Khalimonenko, О. Kupreev // SecureList. – AO Kaspersky Lab., 2017. – Режим доступа: https://securelist.com/ddos-attacks-in-q1-2017/78285/ (дата обращения: 01.04.19)
4. Lindsay Jon R. The Impact of China on Cybersecurity. International Security. 2015, vol. 39, no. 3, p. 153. (In Eng.) Режим доступа: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2849&context=lawreview
5. Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U. S.–China Economic and Security Review Commission [Электронный ресурс] // <https://www.uscc.gov/research/occupying-information-high-ground-chinese-capabilities-computer-network-operations-and> (дата обращения: 05.03.2020).
6. Visa и Mastercard заблокировали карты российского банка [Электронный ресурс] // РИА новости, 2014-2020. – Режим доступа: <https://ria.ru/20190313/1551760480.html>. (дата обращения: 23.03.2020).
7. Yan Sophia. China's new cybersecurity law takes effect today, and many are confused / Sophia Yan // CNBC. 31.05.2017. Режим доступа: https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html (дата обращения: 13.03.2018).
8. Аналитики назвали Россию в числе пяти стран с лучшими кибервойсками [Электронный ресурс] // РБК. АО «РОСБИЗНЕСКОНСАЛТИНГ», 1995-2020. – Режим доступа: https://www.rbc.ru/politics/10/01/2017/58747b439a7947526d203417. (дата обращения: 18.03.2020).
9. Аудитория интернета в России [Электронный ресурс] // Исследовательская компания Mediascope. – Режим доступа: https://webindex.mediascope.net/. (дата обращения: 14.03.2019).
10. Батуева Е.В. К определению национальной киберстратегии [Электронный ресурс] / Е.В. Батуева // Международные процессы. – 2018. - №3. С. 82 – Режим доступа: https://www.elibrary.ru/download/elibrary\_23488866\_62261636.pdf. (дата обращения: 11.03.2020).
11. ВОИС ИС: факты и цифры 2019 год [Электронный ресурс] // WIPO Всемирная организация интеллектуальной собственности. – Режим доступа: https://www.wipo.int/edocs/pubdocs/ru/wipo\_pub\_943\_2019.pdf. (дата обращения: 02.04.2020). – Загл. с экрана.
12. Государственная программа Российской Федерации «Информационное общество (2011 - 2020 годы)», утвержденная распоряжением Правительства Российской Федерации от 20 октября 2010 г. N 1815-р. ИСС Консультант +
13. Доля платежной системы "Мир" по операциям на рынке России достигла 18,6% [Электронный ресурс] // ТАСС, 1999-2020. – Режим доступа: https://tass.ru/ekonomika/6952834. (дата обращения: 23.03.2020).
14. Е. Черненко. Россия зашла в ООН со своим киберуставом [Электронный ресурс]/ Е. Черненко // Газета "Коммерсантъ" №226 от 07.12.2018 - Режим доступа: https://www.kommersant.ru/doc/3821853(дата обращения: 06.05.2019).
15. Импортозамещение программного обеспечения в госсекторе [Электронный ресурс] // Tadviser государство, бизнес, IT. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Импортозамещение\_программного\_обеспечения\_в\_госсекторе. (дата обращения: 23.03.2020).
16. Интернет-торговля рынок России [Электронный ресурс] // Tadviser государство, бизнес, IT. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Интернет-торговля\_(рынок\_России). (дата обращения: 14.03.2020).
17. Итоги федерального статистического наблюдения по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей [Электронный ресурс] // Федеральная служба государственной статистики – Режим доступа: https://www.gks.ru/free\_doc/new\_site/business/it/fed\_nabl-croc/PublishData%5CReports%5CReports\_2016.html. (дата обращения: 23.03.2020).
18. Кибервойска Европы и НАТО [Электронный ресурс] // РСДМ, 2010-2020 – Режим доступа URL: https://russiancouncil.ru/analytics-and-comments/analytics/kibervoyska-evropy-i-nato/ (дата обращения: 05.03.2020).
19. Киберкомандование США US Cybercom [Электронный ресурс] // Tadviser государство, бизнес, IT. – Режим доступа: http://www.tadviser.ru/index.php/Статья: Киберкомандование США US. (дата обращения: 14.03.2020).
20. Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России [Электронный ресурс] // лаборатория касперского – Режим доступа: https://docplayer.ru/393876-Kiberugrozy-i-informacionnaya-bezopasnost-v-korporativnom-sektore-tendencii-v-mire-i-v-rossii.html
21. Китай устроил кибератаку на компании из США и Японии [Электронный ресурс] // РБК. 2015-2020. – Режим доступа https://quote.rbc.ru/news/article/5ae098a62ae5961b67a1c1d1. (дата обращения: 23.03.2020).
22. Ковалев А. А. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока [Электронный ресурс] / А.А. Ковалев, А. И. Балашов // Вестник ПАГС. -2018. - №5. - С. 108. Режим Доступа: https://cyberleninka.ru/article/n/mezhdunarodno-pravovye-aspekty-politiki-kiberbezopasnosti-nekotoryh-evropeyskih-stran-byvshego-sovetskogo-bloka (дата обращения: 20.05.2020).
23. Корнев, М. Суверенная кибербезопасность: как глобальные проблемы влияют на ограничения медиа в интернете? / М. Корнев // Журналист. – 2015. – №02. – ООО Медиагруппа «Журналист», 2019. – Режим доступа: http://mediatoolbox.ru/blog/suverennaya-kiber-bezopasnost-kak-globalnyie-problemyi-vliyayut-na-ogranicheniya-media-v-internete/, свободный. – Загл. с экрана.
24. Кучерявый М.М. Роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации [Электронный ресурс] / М.М. Кучерявый // Известия российского государственного педагогического университета им. А. И. Герцена. — 2014. — №164. — С. 165. — Режим доступа https://www.elibrary.ru/item.asp?id=21585731. (дата обращения: 16.03.2020).
25. Ламинина О.Г. Роль информационной безопасности в политике [Электронный ресурс] / О.Г. Ламинина // Гуманитарный вестник. — 2013. — №4. — С. 5. — Режим доступа https://cyberleninka.ru/article/n/rol-informatsionnoy-bezopasnosti-v-politike/viewer. (дата обращения: 16.03.2020).
26. Лучший из лучших? Как создают мощнейший квантовый компьютер [Электронный ресурс] // Газета.ru от 23.09.2019 Режим доступа: https://www.gazeta.ru/science/2019/09/23\_a\_12670717.shtml (дата обращения: 06.02.2020).
27. О принятии Генассамблеей ООН российской резолюции по международной информационной безопасности [Электронный ресурс] // Министерство иностранных дел Российской Федерации Режим доступа: http://www.mid.ru/foreign\_policy/news//asset\_publisher/cKNonkJE02Bw/content/id/3437775 (дата обращения: 24.03.2019).
28. Пентагон изменил стратегию киберкомандования США [Электронный ресурс] // News.com, 1999-2020. – Режим доступа https://www.newsru.com/world/18jun2018/cyber.html. (дата обращения: 23.03.2020).
29. Разумов Е.А. Политика КНР по обеспечению кибербезопасности [Электронный ресурс] / Е.А. Разумов // Россия и АТР. - 2017. - №4 (98). - С. 158 - Режим доступа: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti (дата обращения: 11.05.2020).
30. Российские процессоры: прошлое, настоящее и будущее [Электронный ресурс] // Zoom 1995-2020. – Режим доступа https://zoom.cnews.ru/publication/item/55734. (дата обращения: 01.04.2020). – Загл. с экрана.
31. США могут отключить Россию от интернета. Как мы защищаемся? [Электронный ресурс] URA.RU, 2004-2020. – Режим доступаhttps://ura.news/articles/1036277337 (дата обращения: 22.03.2020).
32. Толстухина А. Лучше две киберрезолюции, чем ни одной [Электронный ресурс]/ А. Толстухина // РСДМ, Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/luchshe-dve-kiberrezolyutsii-chem-ni-odnoy/(дата обращения: 06.05.2019).

1. См.: Жаглин А. В. Понятийный аппарат теории национальной безопасности/ А.В. Жаглин // Вестник Воронежского института МВД России – 2014. – № 3 – С. 160. [↑](#footnote-ref-1)
2. #  См.: Kerschischnig G. Cyberthreats and International Law. / G. Kerschischnig  - The Hague, 2012. - P. 5.

 [↑](#footnote-ref-2)
3. См.: Ирошников Д. В. Соотношение понятий "опасность", "угроза", "вызов" и "риск" в правовой доктрине, действующем законодательстве и документах стратегического планирования / Ирошников Д. В. // Транспорт, право и безопасность – 2017. – № 12 – С. 97. [↑](#footnote-ref-3)
4. См.: Безкоровайный М.М. Кибербезопасность подходы к определению понятия / М.М. Безкоровайный, А.Л. Татузов // Вопросы кибербезопасности. - 2014. - №1 (2) - С. 22-27. [↑](#footnote-ref-4)
5. См.: Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. д-ра юрид. Наук / М.Б. Касенова. -М., 2016 - С.27 [↑](#footnote-ref-5)
6. См.: Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни / Н.В. Кардава // Каспийский регион: политика, экономика, культура – 2019. – № 3(60). С. 74 [↑](#footnote-ref-6)
7. См.: Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности // Журнал зарубежного законодательства и сравнительного правоведения – 2017. – № 6 – С. 48 [↑](#footnote-ref-7)
8. См.: Паршин С. А. Кибервойны — реальная угроза национальной безопасности / С. А. Паршин, Ю. Е. Горбачев, Ю. А. Кожанов — М.: КРАСАНД, 2011. — 96 с. [↑](#footnote-ref-8)
9. См.: Гриняев С. Н. Поле битвы — киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев — М.: Харвест, 2004. — С. 198-199. [↑](#footnote-ref-9)
10. См.: Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: монография / С.И. Макаренко — СПб.: Наукоемкие технологии, 2017. — с.225-227. [↑](#footnote-ref-10)
11. # См.: Макаров В.Е. (2015). Политические и социальные аспекты информационной безопасности. Монография – Таганрог. Изд. С.А. Ступин

 [↑](#footnote-ref-11)
12. См.: Бухарин С. Н. Методы и технологии информационных войн / С. Н. Бухарин, В. В. Цыганов — М.: Академический проект, 2007. — 382 с. [↑](#footnote-ref-12)
13. См.: Мкртычян А.А. Влияние средств массовой информации на психологические последствия терроризма: автореф. дис. канд. псих. наук. / А.А. Мкртычян – М.: Моск. гос. ун-т им. М.В. Ломоносова, 2012. – С. 37. [↑](#footnote-ref-13)
14. См.: Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017. - с. 81-85. [↑](#footnote-ref-14)
15. Шелкоплясова Н.И. Роль войск информационных операций в защите интересов национальной безопасности / Шелкоплясова Н.И.// [Вестник тульского филиала финуниверситета](https://www.elibrary.ru/contents.asp?id=39560579). - 2019. - № 1. С. 125. [↑](#footnote-ref-15)
16. Душкин Р. В. Обзор текущего состояния квантовых технологий. /Р.В.Душкин// Компьютерные исследования и моделирование 2018 Т. 10 № 2 С. 165 [↑](#footnote-ref-16)
17. Потапов А.С. Технологии искусственного интеллекта /А.С. Потапов – СПб: СПбГУ ИТМО, 2010. С.3 [↑](#footnote-ref-17)
18. Мурзин Ф.А. Облачные технологии: основные понятия, задачи и тенденции развития / Ф.А.Мурзин, Т.В. Батура, Д.Ф Семич. // Программные продукты, системы и алгоритмы. 2014. № 1. С. 64. [↑](#footnote-ref-18)
19. Калашников А.О. новых технологий на информационную безопасность критической информационной инфраструктуры/ А.О. Калашников, Е.В. Аникина // Информация и безопасность – 2019. – № 2 – С. 56. [↑](#footnote-ref-19)
20. Запечников С.В. Проблемы обеспечения информационной безопасности больших данных / С. В. Запечников, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой // Безопасность информационных технологий. 2014. Т. 21. №. 3. С. 9 [↑](#footnote-ref-20)
21. Цветков В.Я. Кибер физические системы /В.Я. Цветков// Международный журнал прикладных и фундаментальных исследований. – 2017. – № 6-1. – С. 64 [↑](#footnote-ref-21)
22. Киберпространство – сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности. [↑](#footnote-ref-22)
23. Кедровский О.В. Информационное пространство России / О.В.Кедровский // Информационные ресурсы России. —1994. — № 4. — C. 2—3. [↑](#footnote-ref-23)
24. Федеральный закон от 3 апреля 2005 года N 149 " Об информации, информационных технологиях и о защите информации " [Электронный ресурс] // Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения: 17.04.202020). [↑](#footnote-ref-24)
25. Философский словарь / Под ред. И.Т. Фролова. — М.: Республика, 2001. — С. 356 [↑](#footnote-ref-25)
26. Дзялошинский, И. М. Информационное пространство России: структура, особенности функционирования, перспективы эволюции / И. М. Дзялошинский. – Моск. центр Карнеги, М.: – 2001. – 30 с [↑](#footnote-ref-26)
27. Лихтин А.А. Теоретические аспекты понятия «информационная политика» и особенности ее реализации в современной российской общественно-политической реальности /А.А. Лихтин, А.А. Ковалев// Управленческое консультирование. — 2017. — №1 (97). — С. 32 [↑](#footnote-ref-27)
28. См.: Лазарев И.А. Информация и безопасность. Композиционная технология. М.: Изд-во Московского городского центра научно-технической информации, 2002. [↑](#footnote-ref-28)
29. См.: Лопатин В.Н. Информационная безопасность России: человек, общество, государство / В.Н. Лопатин // Серия: Безопасность человека и общества. СПб.: Фонд Университет, 2000. С. 428. [↑](#footnote-ref-29)
30. См.: Уфимцев Ю.С., Ерофеев Е.А. и др. Информационная безопасность России. М.: Экзамен, 2003. [↑](#footnote-ref-30)
31. Чеботарева А.А., Научные подходы к определению понятия "информационная безопасность" / А.А. Чеботарева // Информационное право – 2011. - №1. С. 3-6. [↑](#footnote-ref-31)
32. Атаманов Г.А. Информационная безопасность: сущность и содержание / Г.А. Атаманов // Бизнес и безопасность в России. - 2007. - N 47. - С. 108. [↑](#footnote-ref-32)
33. Проценко Е.А. Модель и метод анализа эффективности систем защиты информации сайтов органов власти Российской Федерации: Автореф. дис. канд. технич. наук. / Е.А. Проценко - СПб., 2008. [↑](#footnote-ref-33)
34. Лопатин В.Н. Информационная безопасность России: человек, общество, государство / В.Н. Лопатин // Серия: Безопасность человека и общества. СПб.: Фонд Университет, 2000. - С. 428. [↑](#footnote-ref-34)
35. Стрельцов А.А. Содержание понятия "обеспечение информационной безопасности" // Информационное общество. - 2001. - №. 4. - С. 16. [↑](#footnote-ref-35)
36. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // ФГБУ «Редакция «Российской газеты», 1998-2020. – Режим доступа: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>. (дата обращения: 17.03.2020). – Загл. с экрана. [↑](#footnote-ref-36)
37. См., например, Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ; Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ (ред. от 28.04.2015 г.) // СПС Консультант плюс. [↑](#footnote-ref-37)
38. Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. д-ра юрид. Наук / М.Б. Касенова. -М., 2016 - С.27 [↑](#footnote-ref-38)
39. См., например: Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни / Н.В. Кардава // Каспийский регион: политика, экономика, культура – 2019. – № 3(60). С. 74; Cyber Security Strategy for Germany (2011) [Электронный ресурс] // Federal Ministry of the Interior – Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-Germany (дата обращения: 05.03.2020); Киберпространство БРИКС: правовое измерение: монография. М., 2017. [↑](#footnote-ref-39)
40. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений. — 4-е изд., М., 1997. — 944 с. [↑](#footnote-ref-40)
41. См.: Wellman B. Physical place and cyberplace: the rise of personalized networking // International Journal of Urban and Regional Research. 2001. Vol. 25 (2). P. 247. [↑](#footnote-ref-41)
42. См.: Войскунский А.Е. Метафоры интернета / А.Е. Войкунский // Вопросы философии. 2001. № 11. С. 64–79. [↑](#footnote-ref-42)
43. См.: Ploug T. Ethic sin cyberspace: how cyberspace may influence interpersonal interaction. Dordrecht, 2009. P. 69–70. [↑](#footnote-ref-43)
44. Жаглин А. В. Понятийный аппарат теории национальной безопасности/ А.В Жаглин // Вестник Воронежского института МВД России – 2014. – № 3 – С. 160. [↑](#footnote-ref-44)
45. Ирошников Д. В. Соотношение понятий "опасность", "угроза", "вызов" и "риск" в правовой доктрине, действующем законодательстве и документах стратегического планирования/ Д.В. Ирошников // Транспорт, право и безопасность – 2017. – № 12 – С. 97. [↑](#footnote-ref-45)
46. A national cyber security strategy (2016) [Электронный ресурс] // Government offices of Sweden – Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy (дата обращения: 07.03.2020). [↑](#footnote-ref-46)
47. Cyber Security Strategy for Germany (2011) [Электронный ресурс] // Federal Ministry of the Interior – Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany (дата обращения: 05.03.2020). [↑](#footnote-ref-47)
48. #  См.: Kerschischnig G. Cyberthreats and International Law. / G. Kerschischnig - The Hague, 2012. - P. 5.

 [↑](#footnote-ref-48)
49. Капустин А.Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности / А.Я. Капустин // Журнал зарубежного законодательства и сравнительного правоведения – 2017. – № 6 – С. 48 [↑](#footnote-ref-49)
50. Марков А.С. Руководящие указания по кибербезопасности в контексте ISO 27032 / А.С. Марков, В. Л. Цирлов // Вопросы кибербезопасности. 2014. №1 (2). URL: https://cyberleninka.ru/article/n/rukovodyaschie-ukazaniya-po-kiberbezopasnosti-v-kontekste-iso-27032 (дата обращения: 23.05.2020). [↑](#footnote-ref-50)
51. Зубарев И.В. Кибербезопасность автоматизированных систем управления военного назначения / И.В. Зубарев, И.В. Жидков, И.В. Кадушкин // Вопросы кибербезопасности. - 2013. - № 1(1). - 12 с. [↑](#footnote-ref-51)
52. #  См., например: Киберугрозы и информационная безопасность в корпоративном секторе: тенденции в мире и в России [Электронный ресурс] // лаборатория касперского – Режим доступа: https://docplayer.ru/393876-Kiberugrozy-i-informacionnaya-bezopasnost-v-korporativnom-sektore-tendencii-v-mire-i-v-rossii.html

 [↑](#footnote-ref-52)
53. Калашников А.О. новых технологий на информационную безопасность критической информационной инфраструктуры/ А.О. Калашников, Е.В. Аникина // Информация и безопасность – 2019. – № 2 – С. 56. [↑](#footnote-ref-53)
54. Там же. [↑](#footnote-ref-54)
55. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // ФГБУ «Редакция «Российской газеты», 1998-2020. – Режим доступа: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>. (дата обращения: 17.03.2020). – Загл. с экрана. [↑](#footnote-ref-55)
56. Анализ текущего состояния развития цифровой экономики в России. М.: Институт развития информационного общества, 2018. — С. 50. [↑](#footnote-ref-56)
57. Государственная программа Российской Федерации «Информационное общество (2011 - 2020 годы)», утвержденная распоряжением Правительства Российской Федерации от 20 октября 2010 г. N 1815-р. ИСС Консультант + [↑](#footnote-ref-57)
58. Там же. [↑](#footnote-ref-58)
59. Гуцев М.В. Диверсификация на высокотехнологичных предприятиях / М.В. Гуцев // Журнал Актуальные проблемы гуманитарных и естественных наук. – 2019. – №10/2011 – С.13. [↑](#footnote-ref-59)
60. Шишкина Т.С. Преимущества и недостатки внедрения стратегии диверсификации / Т.С. Шишкина // Актуальные проблемы экономики современной России. - 2015. - № 2. - С. 339-348. [↑](#footnote-ref-60)
61. Анализ текущего состояния развития цифровой экономики в России. М.: Институт развития информационного общества, 2018. — С. 50-56. [↑](#footnote-ref-61)
62. Душкин Р. В. Обзор текущего состояния квантовых технологий. / Р.В. Душкин // Компьютерные исследования и моделирование – 2018. - Т. 10 - № 2 - С. 165 [↑](#footnote-ref-62)
63. Янковская Ю. Ю. Стойкость квантовых протоколов распределения ключей / Ю.Ю. Янковская, А. А. Марина // Сomputer sciences and telecommunications — 2013. — C. 2 [↑](#footnote-ref-63)
64. Душкин Р. В. Обзор текущего состояния квантовых технологий / Р.В. Душкин // Компьютерные исследования и моделирование 2018 Т. 10 № 2 С. 167 [↑](#footnote-ref-64)
65. ##  Лучший из лучших? Как создают мощнейший квантовый компьютер [Электронный ресурс] // Газета.ru от 23.09.2019 Режим доступа: https://www.gazeta.ru/science/2019/09/23\_a\_12670717.shtml (дата обращения: 06.02.2020).

 [↑](#footnote-ref-65)
66. Потапов А.С. Технологии искусственного интеллекта / А.С. Потапов – СПб: СПбГУ ИТМО, 2010. С.3 [↑](#footnote-ref-66)
67. Мурзин Ф.А. Облачные технологии: основные понятия, задачи и тенденции развития / Ф.А. Мурзин, Т.В. Батура, Д.Ф Семич // Программные продукты, системы и алгоритмы. - 2014. - № 1. - С. 64. [↑](#footnote-ref-67)
68. Калашников А.О. новых технологий на информационную безопасность критической информационной инфраструктуры/ А.О. Калашников, Е.В. Аникина // Информация и безопасность – 2019. – № 2 – С. 56. [↑](#footnote-ref-68)
69. Запечников С.В. Проблемы обеспечения информационной безопасности больших данных / С. В. Запечников, Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой // Безопасность информационных технологий. - 2014. - Т. 21. - №. 3. - С. 9 [↑](#footnote-ref-69)
70. Там же. [↑](#footnote-ref-70)
71. Цветков В.Я. Кибер физические системы / В. Я. Цветков // Международный журнал прикладных и фундаментальных исследований. – 2017. – № 6-1. – С. 64 [↑](#footnote-ref-71)
72. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" [↑](#footnote-ref-72)
73. Там же. [↑](#footnote-ref-73)
74. Капустин А. Я. К вопросу о международно-правовой концепции угроз международной информационной безопасности / А. Я. Капустин // Журнал зарубежного законодательства и сравнительного правоведения – 2017. – № 6 – С. 45 [↑](#footnote-ref-74)
75. Касенова М. Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. д-ра юрид. Наук / М.Б. Касенова. -М., 2016 - С.27 [↑](#footnote-ref-75)
76. Khalimonenko, А. DDOS attacks in Q1 2017 [Электронный ресурс] /А. Khalimonenko, О. Kupreev // SecureList. – AO Kaspersky Lab., 2017. – Режим доступа: https://securelist.com/ddos-attacks-in-q1-2017/78285/ (дата обращения: 01.04.19) [↑](#footnote-ref-76)
77. Declaration by the Committee of Ministers on Internet Governance Principles [Электронный ресурс]// Committee of Ministers on Internet Governance. – 2011. – Режим доступа: https://wcd.coe. int/ViewDoc.jsp?id=1835773 (дата обращения: 01.04.19) [↑](#footnote-ref-77)
78. ###  Резолюция ГА ООН A/RES/56/19 от 29 ноября 2001 г. // Режим доступа: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf (дата обращения: 24.03.2019).

 [↑](#footnote-ref-78)
79. ###  О принятии Генассамблеей ООН российской резолюции по международной информационной безопасности [Электронный ресурс] // Министерство иностранных дел Российской Федерации Режим доступа: http://www.mid.ru/foreign\_policy/news//asset\_publisher/cKNonkJE02Bw/content/id/3437775 (дата обращения: 24.03.2019).

 [↑](#footnote-ref-79)
80. ###  Резолюция ГА ООН 73/27 от 5 декабря 2018 [Электронный ресурс] // ГЕНЕРАЛЬНАЯ АССАМБЛЕЯ ООН Режим доступа: https://undocs.org/ru/A/RES/73/27 (дата обращения: 24.03.2019).

 [↑](#footnote-ref-80)
81. ###  Там же.

 [↑](#footnote-ref-81)
82. ##  Е. Черненко. Россия зашла в ООН со своим киберуставом [Электронный ресурс]/ Е. Черненко // Газета "Коммерсантъ" №226 от 07.12.2018 - Режим доступа: https://www.kommersant.ru/doc/3821853(дата обращения: 06.05.2019).

 [↑](#footnote-ref-82)
83. ###  О принятии Генассамблеей ООН российской резолюции по международной информационной безопасности [Электронный ресурс] // Министерство иностранных дел Российской Федерации Режим доступа: http://www.mid.ru/foreign\_policy/news//asset\_publisher/cKNonkJE02Bw/content/id/3437775 (дата обращения: 24.03.2019).

 [↑](#footnote-ref-83)
84. ###  Резолюция ГА ООН 73/266 от 22 декабря 2018 [Электронный ресурс] // ГЕНЕРАЛЬНАЯ АССАМБЛЕЯ ООН Режим доступа: https://www.un.org/en/ga/search/view\_doc.asp?symbol=A/RES/73/266&Lang=R (дата обращения: 24.03.2019).

 [↑](#footnote-ref-84)
85. ##  А. Толстухина. Лучше две киберрезолюции, чем ни одной [Электронный ресурс]/ А. Толстухина // РСДМ, Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/luchshe-dve-kiberrezolyutsii-chem-ni-odnoy/(дата обращения: 06.05.2019).

 [↑](#footnote-ref-85)
86. Clinton William. National Security Strategy / Washington DC: Government Printing Office. February 1995. P. 8. [↑](#footnote-ref-86)
87. The National Strategy to Secure Cyber Space / The White House, Washington DC, USA, 2003 // The White House. 2003. Режим доступа: http://georgewbush-whitehouse.archives.gov/pcipb/ (дата обращения: 25.02.2018). [↑](#footnote-ref-87)
88. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection. // U.S. Department of Homeland Security. 17.12.2003. Режим доступа: https://www.dhs.gov/homeland-security-presidential-directive-7 (дата обращения: 25.02.2020). [↑](#footnote-ref-88)
89. The Comprehensive National Cybersecurity Initiative [Электронный ресурс] // The White House. – 2008- Режим доступа: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurityinitiative (дата обращения: 15.05.2020). [↑](#footnote-ref-89)
90. Пентагон изменил стратегию киберкомандования США [Электронный ресурс] // News.com, 1999-2020. – Режим доступа https://www.newsru.com/world/18jun2018/cyber.html. (дата обращения: 23.03.2020). [↑](#footnote-ref-90)
91. U.S. Cyber Command’s Malware Inoculation: Linking Offense and Defense in Cyberspace [Электронный ресурс] // Council of foreign relation. – Режим доступа https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace. (дата обращения: 23.03.2020). [↑](#footnote-ref-91)
92. Cyber Strategy 2018 [Электронный ресурс] / Department of Defense Summary – 2018 - Режим доступа: https://media.defense.gov/2018/ Sep/18/2002041658/-1/-1/1/CYBER\_STRATEGY\_SUMMARY\_FINAL.PDF (дата обращения: 01.10.2018). [↑](#footnote-ref-92)
93. Cybersecurity and Infrastructure Security Agency Act of 2018 [Электронный ресурс] // The White House. – Режим доступа: https://www.congress.gov/bill/115th-congress/house-bill/3359 (дата обращения: 15.05.2020). [↑](#footnote-ref-93)
94. Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая: автореф. дис. канд. полит. наук. / Е.В. Батуева – М.: МГИМО, 2014. – С. 50. [↑](#footnote-ref-94)
95. Разумов Е.А. Политика КНР по обеспечению кибербезопасности [Электронный ресурс] / Е.А. Разумов // Россия и АТР. 2017. №4 (98). С. 158 Режим доступа: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti (дата обращения: 11.05.2020). [↑](#footnote-ref-95)
96. Национальная оборона Китая в 2002 году [Электронный ресурс] // Информационное бюро Государственного совета Народной Республики Китай. - 2002. - Режим доступа: http://www.scio.gov.cn/zfbps/ndhf/2002/Document/307925/307925.htm (дата обращения: 11.05.2020). [↑](#footnote-ref-96)
97. Разумов Е.А. Политика КНР по обеспечению кибербезопасности [Электронный ресурс] / Е.А. Разумов // Россия и АТР. 2017. №4 (98). С. 158 Режим доступа: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti (дата обращения: 11.05.2020). [↑](#footnote-ref-97)
98. Ventre D. Chinese Cybersecurity and Defense. London / D. Ventre // Wiley­ISTE Publ., - 2014. - 301 p. [↑](#footnote-ref-98)
99. Разумов Е.А. Политика КНР по обеспечению кибербезопасности [Электронный ресурс] / Е.А. Разумов // Россия и АТР. 2017. №3. С. 159. Режим доступа: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti (дата обращения: 11.05.2020). [↑](#footnote-ref-99)
100. Yan S. China's new cybersecurity law takes effect today, and many are confused / S. Yan // CNBC. - 2017. - Режим доступа: https://www.cnbc.com/2017/05/31/chinas-new-cybersecurity-law-takes-effect-today.html (дата обращения: 13.03.2018). [↑](#footnote-ref-100)
101. Lindsay J. R. The Impact of China on Cybersecurity / J.R. Lindsay // International Security. – 2015. - vol. 39. - p. 153. - Режим доступа: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2849&context=lawreview [↑](#footnote-ref-101)
102. Рогожин А.А. КНР – Закон о кибербезопасности принят [Электронный ресурс] / А.А. Рогожин – Режим доступа: https://www.imemo.ru/news/events/text/knr-zakon-o-kiberbezopasnosti-prinyat. (дата обращения: 20.04.2020). [↑](#footnote-ref-102)
103. Там же. [↑](#footnote-ref-103)
104. Там же. [↑](#footnote-ref-104)
105. Разумов Е.А. Политика КНР по обеспечению кибербезопасности [Электронный ресурс] / Е.А. Разумов// Россия и АТР. 2017. №4 (98). С. 158 Режим доступа: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti (дата обращения: 11.05.2020). [↑](#footnote-ref-105)
106. См.: Разумов Е.А. Политика КНР по обеспечению кибербезопасности [Электронный ресурс] / Е.А, Разумов // Россия и АТР. 2017. №4 (98). С. 157-168 Режим доступа: https://cyberleninka.ru/article/n/politika-knr-po-obespecheniyu-kiberbezopasnosti (дата обращения: 11.05.2020). [↑](#footnote-ref-106)
107. См.: Иб­ра­ги­мо­ва Г. Стра­те­гия КНР в ки­бер­про­стран­ст­ве: во­про­сы управ­ле­ния ин­терне­том и обес­пе­че­ние ин­фор­ма­ци­он­ной безо­пас­но­сти // Ин­декс безо­пас­но­сти. 2013. № 1 (104). С.169—184. [↑](#footnote-ref-107)
108. Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage. Prepared for the U. S.–China Economic and Security Review Commission [Электронный ресурс] // <https://www.uscc.gov/research/occupying-information-high-ground-chinese-capabilities-computer-network-operations-and> (дата обращения: 05.03.2020). [↑](#footnote-ref-108)
109. Китай устроил кибератаку на компании из США и Японии [Электронный ресурс] // РБК. 2015-2020. – Режим доступа https://quote.rbc.ru/news/article/5ae098a62ae5961b67a1c1d1. (дата обращения: 23.03.2020). [↑](#footnote-ref-109)
110. Global Cybersecurity Index (GCI) (2018) [Электронный ресурс] // International Telecommunication Union – Режим доступа: https://www.itu.int/dms\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (дата обращения: 05.03.2020). [↑](#footnote-ref-110)
111. См., например: Умерова И.А. Экономические связи между странами-членами ЕС как фактор регионального единства и развития: диссертация кандидата экономических наук / И.А. Разумова Российский университет дружбы народов, Москва, 2009. [↑](#footnote-ref-111)
112. Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни / Н.В. Кардава //Каспийский регион: политика, экономика, культура – 2019. – № 3(60). С. 74-76. [↑](#footnote-ref-112)
113. Convention on Cybercrime, Budapest, 2001 [Электронный ресурс] // Official web-site of Council of Europe. Режим доступа: http:// conventions.coe.int./Treaty/en/Treaties/Html/185.htm (дата обращения: 17.05.2020). [↑](#footnote-ref-113)
114. Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни / Н.В. Кардава //Каспийский регион: политика, экономика, культура – 2019. – № 3(60). С. 74-76. [↑](#footnote-ref-114)
115. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [Электронный ресурс] // Brussels, 7.2.2013 JOIN (2013) 1 final Режим доступа: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec\_comm\_en.pdf (дата обращения: 17.05.2020). [↑](#footnote-ref-115)
116. EUROPEAN CYBERCRIME CENTRE - EC3 [Электронный ресурс] // Europol Режим доступа: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (дата обращения: 17.05.2020). [↑](#footnote-ref-116)
117. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [Электронный ресурс] // Official Journal of the European Union. Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC (дата обращения: 17.05.2020). [↑](#footnote-ref-117)
118. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [Электронный ресурс] // Official Journal of the European Union.: http://data.europa.eu/eli/reg/2016/679/oj (дата обращения: 17.05.2020). [↑](#footnote-ref-118)
119. Ковалев А. А. Международно-правовые аспекты политики кибербезопасности некоторых европейских стран бывшего советского блока [Электронный ресурс] / А.А. Ковалев, А. И. Балашов // Вестник ПАГС. -2018. - №5. - С. 108. Режим Доступа: https://cyberleninka.ru/article/n/mezhdunarodno-pravovye-aspekty-politiki-kiberbezopasnosti-nekotoryh-evropeyskih-stran-byvshego-sovetskogo-bloka (дата обращения: 20.05.2020). [↑](#footnote-ref-119)
120. См., например, Директива (ЕС) № 2016/1148. [↑](#footnote-ref-120)
121. Cyber Security Strategy for Germany (2011) [Электронный ресурс] // Federal Ministry of the Interior – Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany (дата обращения: 05.03.2020). [↑](#footnote-ref-121)
122. Там же. [↑](#footnote-ref-122)
123. Там же. [↑](#footnote-ref-123)
124. Там же. [↑](#footnote-ref-124)
125. Там же. [↑](#footnote-ref-125)
126. Там же. [↑](#footnote-ref-126)
127. Кибервойска Европы и НАТО [Электронный ресурс] // РСДМ, 2010-2020 – Режим доступа: https://russiancouncil.ru/analytics-and-comments/analytics/kibervoyska-evropy-i-nato/ (дата обращения: 05.03.2020). [↑](#footnote-ref-127)
128. Austrian Cyber Security Strategy (2013) [Электронный ресурс – Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy (дата обращения: 07.03.2020). [↑](#footnote-ref-128)
129. Кардава Н.В. Политика обеспечения кибербезопасности в европейском союзе: национальный и наднациональный уровни / Н.В. Кардава //Каспийский регион: политика, экономика, культура – 2019. – № 3(60). С. 74. [↑](#footnote-ref-129)
130. Там же. [↑](#footnote-ref-130)
131. Global Positioning System —[спутниковая система навигации](https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D1%83%D1%82%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D0%BD%D0%B0%D0%B2%D0%B8%D0%B3%D0%B0%D1%86%D0%B8%D0%B8), обеспечивающая измерение расстояния, времени и определяющая местоположение во всемирной системе координат. [↑](#footnote-ref-131)
132. Кибертерроризм - политически мотивированное преступление государственных и / или негосударственных субъектов против компьютеров, сетей и хранящейся в них информации.  (Austrian Cyber Security Strategy. 2013 г.). [↑](#footnote-ref-132)
133. Кибервойна - акты войны в виртуальном пространстве и вокруг него с помощью средств, которые преимущественно связаны с информационными технологиями.  (Austrian Cyber Security Strategy. 2013 г.). [↑](#footnote-ref-133)
134. Кибератака - атака в киберпространстве, которая направлена против

одной или нескольких ИТ-систем.  (Austrian Cyber Security Strategy. 2013 г.). [↑](#footnote-ref-134)
135. Киберпреступность - незаконные атаки из киберпространства на системы ИКТ или через них.  (Austrian Cyber Security Strategy. 2013 г.). [↑](#footnote-ref-135)
136. Кибершпионаж - кибератаки, направленные против конфиденциальности ИТ-системы (Austrian Cyber Security Strategy. 2013 г.). [↑](#footnote-ref-136)
137. Global Cybersecurity Index (GCI) (2018) [Электронный ресурс] // International Telecommunication Union – Режим доступа: https://www.itu.int/dms\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (дата обращения: 05.03.2020). [↑](#footnote-ref-137)
138. A national cyber security strategy (2016) [Электронный ресурс] // Government offices of Sweden – Режим доступа: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/swedish-national-cyber-security-strategy (дата обращения: 07.03.2020). [↑](#footnote-ref-138)
139. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // ФГБУ «Редакция «Российской газеты», 1998-2020. – Режим доступа: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>. (дата обращения: 17.03.2020). – Загл. с экрана. [↑](#footnote-ref-139)
140. Там же. [↑](#footnote-ref-140)
141. Там же. [↑](#footnote-ref-141)
142. Кучерявый М.М. Роль информационной составляющей в системе политики обеспечения национальной безопасности Российской Федерации [Электронный ресурс] / М.М. Кучерявый // Известия российского государственного педагогического университета им. А. И. Герцена. — 2014. — №164. — С. 165. — Режим доступа https://www.elibrary.ru/item.asp?id=21585731. (дата обращения: 16.03.2020). [↑](#footnote-ref-142)
143. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // ФГБУ «Редакция «Российской газеты», 1998-2020. – Режим доступа: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>. (дата обращения: 17.03.2020). – Загл. с экрана. [↑](#footnote-ref-143)
144. Там же. [↑](#footnote-ref-144)
145. Аудитория интернета в России [Электронный ресурс] // Исследовательская компания Mediascope. – Режим доступа: https://webindex.mediascope.net/. (дата обращения: 14.03.2019). [↑](#footnote-ref-145)
146. Интернет-торговля рынок России [Электронный ресурс] // Tadviser государство, бизнес, IT. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Интернет-торговля\_(рынок\_России). (дата обращения: 14.03.2020). [↑](#footnote-ref-146)
147. Там же. [↑](#footnote-ref-147)
148. Ламинина О.Г. Роль информационной безопасности в политике [Электронный ресурс] / О.Г. Ламинина // Гуманитарный вестник. — 2013. — №4. — С. 5. — Режим доступа https://cyberleninka.ru/article/n/rol-informatsionnoy-bezopasnosti-v-politike/viewer. (дата обращения: 16.03.2020). [↑](#footnote-ref-148)
149. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // ФГБУ «Редакция «Российской газеты», 1998-2020. – Режим доступа: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>. (дата обращения: 17.03.2020). – Загл. с экрана. [↑](#footnote-ref-149)
150. #  Киберкомандование США US Cybercom [Электронный ресурс] // Tadviser государство, бизнес, IT. – Режим доступа: http://www.tadviser.ru/index.php/Статья: Киберкомандование США US. (дата обращения: 14.03.2020).

 [↑](#footnote-ref-150)
151. Аналитики назвали Россию в числе пяти стран с лучшими кибервойсками [Электронный ресурс] // РБК. АО «РОСБИЗНЕСКОНСАЛТИНГ», 1995-2020. – Режим доступа: https://www.rbc.ru/politics/10/01/2017/58747b439a7947526d203417. (дата обращения: 18.03.2020). [↑](#footnote-ref-151)
152. #  Там же.

 [↑](#footnote-ref-152)
153. Шелкоплясова Н.И. Роль войск информационных операций в защите интересов национальной безопасности / Н.И. Шелкоплясова // [Вестник тульского филиала финуниверситета](https://www.elibrary.ru/contents.asp?id=39560579). - 2019. - № 1. С. 125. [↑](#footnote-ref-153)
154. Аналитики назвали Россию в числе пяти стран с лучшими кибервойсками [Электронный ресурс] // РБК. АО «РОСБИЗНЕСКОНСАЛТИНГ», 1995-2020. – Режим доступа: https://www.rbc.ru/politics/10/01/2017/58747b439a7947526d203417. (дата обращения: 18.03.2020). [↑](#footnote-ref-154)
155. См.: Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017. с. 81-85. [↑](#footnote-ref-155)
156. #  Там же.

 [↑](#footnote-ref-156)
157. #  Там же.

 [↑](#footnote-ref-157)
158. #  Там же.

 [↑](#footnote-ref-158)
159. #  Там же.

 [↑](#footnote-ref-159)
160. Мкртычян А.А. Влияние средств массовой информации на психологические последствия терроризма: автореф. дис. канд. псих. наук. / А.А. Мкртычян – М.: Моск. гос. ун-т им. М.В. Ломоносова, 2012. – С. 37. [↑](#footnote-ref-160)
161. Жаворонкова Т.В Использование сети интернет террористическими и экстремистскими организациями / Т.В. Жаворонкова // Вестник Оренбургского государственного университета – 2015. – № 3 – С. 35. [↑](#footnote-ref-161)
162. Мкртычян А.А. Влияние средств массовой информации на психологические последствия терроризма: автореф. дис. канд. псих. наук. / А.А. Мкртычян – М.: Моск. гос. ун-т им. М.В. Ломоносова, 2012. – С. 37. [↑](#footnote-ref-162)
163. Киберпреступность и киберконфликты: Россия [Электронный ресурс] // Tadviser государство, бизнес, IT. – Режим доступа: http://www.tadviser.ru/index.php/Статья: Киберпреступность и киберконфликты : Россия.(дата обращения: 20.03.2020). [↑](#footnote-ref-163)
164. #  Там же.

 [↑](#footnote-ref-164)
165. #  Корнев, М. Суверенная кибербезопасность: как глобальные проблемы влияют на ограничения медиа в интернете? / М. Корнев // Журналист. – 2015. – №02. – ООО Медиагруппа «Журналист», 2019. – Режим доступа: http://mediatoolbox.ru/blog/suverennaya-kiber-bezopasnost-kak-globalnyie-problemyi-vliyayut-na-ogranicheniya-media-v-internete/, свободный. – Загл. с экрана.

 [↑](#footnote-ref-165)
166. #  Концепция внешней политики Российской Федерации (утв. Президентом РФ 30.11.2016). [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_172989/bc3ab3b04947fc07f452721c58aacccf873d06b6/ (дата обращения: 21.03.2020).

 [↑](#footnote-ref-166)
167. #  Концепция внешней политики Российской Федерации (утв. Президентом РФ 30.11.2016). [Электронный ресурс]. Режим доступа: https://www.mid.ru/foreign\_policy/official\_documents/ /asset\_publisher/CptICkB6BZ29/content/id/2542248 (дата обращения: 21.03.2020).

 [↑](#footnote-ref-167)
168. #  Мягкая сила - способность влиять на другие государства с целью реализации собственных целей через сотрудничество в определенных сферах, направленное на убеждение и формирование положительного восприятия (Nye, Joseph. The Future of Power, 2011).

 [↑](#footnote-ref-168)
169. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // ФГБУ «Редакция «Российской газеты», 1998-2020. – Режим доступа: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>. (дата обращения: 17.03.2020). – Загл. с экрана. [↑](#footnote-ref-169)
170. США могут отключить Россию от интернета. Как мы защищаемся? [Электронный ресурс] URA.RU, 2004-2020.– Режим доступаhttps://ura.news/articles/1036277337 (дата обращения: 22.03.2020). [↑](#footnote-ref-170)
171. #  Федеральный закон от 01.05.2019 N 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации" [Электронный ресурс] // Консультант плюс. – Режим доступа: http://www.consultant.ru/document/cons\_doc\_LAW\_323815/ (дата обращения: 24.03.2019).

 [↑](#footnote-ref-171)
172. #  Криптовалюта - вид цифрового финансового актива, создаваемый и учитываемый в распределенном реестре цифровых транзакций участниками этого реестра в соответствии с правилами ведения реестра цифровых транзакций.

 [↑](#footnote-ref-172)
173. #  Федеральный закон (проект) № 419059-7 "О цифровых финансовых активах" [Электронный ресурс] // Инфо-Бухгалтер. – Режим доступа: https://www.ib.ru/law/81/ (дата обращения: 24.03.2020).

 [↑](#footnote-ref-173)
174. #  ICO - форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной эмиссией.

 [↑](#footnote-ref-174)
175. #  Там же.

 [↑](#footnote-ref-175)
176. См., например: Бухарин С. Н. Методы и технологии информационных войн. /С.Н. Бухарин, В.В. Цыганов — М.: Академический проект, 2007. — 382 с. [↑](#footnote-ref-176)
177. Концепция стратегии кибербезопасности российской федерации (проект) [Электронный ресурс] // Совет Федерации Федерального Собрания Российской Федерации. – Режим доступа: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf. (дата обращения: 22.03.2020). – Загл. с экрана. [↑](#footnote-ref-177)
178. Information Warfare: Department of Defense Directive. TS 3600.1. December 21, 1992 [Электронный ресурс]. – Режим доступа: http://www.dod.mil/pubs/foi/administration\_and\_Management/admin\_matters/14-F0492\_doc\_01\_Directive\_TS-3600-1.pdf (дата обращения: 29.03.2020). [↑](#footnote-ref-178)
179. #  Макаров В.Е. Политические и социальные аспекты информационной безопасности: Монография / В.Е. Макаров. Таганрог. Изд. С.А. Ступин. 2006. – с.105.

 [↑](#footnote-ref-179)
180. См., например,: Паршин С. А. Кибервойны — реальная угроза национальной безопасности / С. А. Паршин, Ю. Е. Горбачев, Ю. А. Кожанов — М.: КРАСАНД, 2011. — 96 с. [↑](#footnote-ref-180)
181. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века: Монография / С.И. Макаренко — СПб.: Наукоемкие технологии, 2017. — с.225-227. [↑](#footnote-ref-181)
182. #  Там же.

 [↑](#footnote-ref-182)
183. Гриняев С. Н. Поле битвы — киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев — М.: Харвест, 2004. — С. 198-199. [↑](#footnote-ref-183)
184. Паршин С. А. Кибервойны — реальная угроза национальной безопасности / С. А. Паршин, Ю. Е. Горбачев, Ю. А. Кожанов — М.: КРАСАНД, 2011. — 96 с [↑](#footnote-ref-184)
185. Импортозамещение программного обеспечения в госсекторе [Электронный ресурс] // Tadviser государство, бизнес, IT. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Импортозамещение\_программного\_обеспечения\_в\_госсекторе. (дата обращения: 23.03.2020). [↑](#footnote-ref-185)
186. Доля платежной системы "Мир" по операциям на рынке России достигла 18,6% [Электронный ресурс] // ТАСС, 1999-2020. – Режим доступа: https://tass.ru/ekonomika/6952834. (дата обращения: 23.03.2020). [↑](#footnote-ref-186)
187. См., например: Visa и Mastercard заблокировали карты российского банка [Электронный ресурс] // РИА новости, 2014-2020. – Режим доступа: <https://ria.ru/20190313/1551760480.html>. (дата обращения: 23.03.2020). [↑](#footnote-ref-187)
188. Государственная программа Российской Федерации «Информационное общество (2011 - 2020 годы)», утвержденная распоряжением Правительства Российской Федерации от 20 октября 2010 г. N 1815-р. ИСС Консультант +. [↑](#footnote-ref-188)
189. Итоги федерального статистического наблюдения по вопросам использования населением информационных технологий и информационно-телекоммуникационных сетей [Электронный ресурс] // Федеральная служба государственной статистики – Режим доступа: https://www.gks.ru/free\_doc/new\_site/business/it/fed\_nabl-croc/PublishData%5CReports%5CReports\_2016.html. (дата обращения: 23.03.2020). [↑](#footnote-ref-189)
190. См., например, Доктрина информационной безопасности Российской Федерации [Электронный ресурс] // ФГБУ «Редакция «Российской газеты», 1998-2020. – Режим доступа: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html>. (дата обращения: 01.04.2020). – Загл. с экрана. [↑](#footnote-ref-190)
191. Российские процессоры: прошлое, настоящее и будущее [Электронный ресурс] // Zoom 1995-2020. – Режим доступа https://zoom.cnews.ru/publication/item/55734. (дата обращения: 01.04.2020). – Загл. с экрана. [↑](#footnote-ref-191)
192. ВОИС ИС: факты и цифры 2019 год [Электронный ресурс] // WIPO Всемирная организация интеллектуальной собственности. – Режим доступа: https://www.wipo.int/edocs/pubdocs/ru/wipo\_pub\_943\_2019.pdf. (дата обращения: 02.04.2020). – Загл. с экрана. [↑](#footnote-ref-192)