# КИБЕРБЕЗОПАСНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ. МОДНЫЙ ТЕРМИН ИЛИ ПРИОРИТЕТНОЕ ТЕХНОЛОГИЧЕСКОЕ НАПРАВЛЕНИЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ XXI ВЕКА

***Добродеев А. Ю.***[1]

***Цель статьи:*** *изучение роли и значения кибербезопасности на современном этапе мирового развития как основного фактора обеспечения национальной и международной безопасности XXI века.*

***Метод исследования:*** *синтез и научное прогнозирование, экспертная оценка, компаративный анализ киберсферы в рамках системного подхода.*

***Результат:*** *кратко проанализированы состояние и пути развития кибербезопасности ведущих зарубежных стран на примере США, состояние и пути развития кибербезопасности и технологии кибербезопасности в Российской Федерации. Представлены с обоснованием дискуссионные предложения по раскрытию термина и понятия «кибербезопасность». В основу раскрытия термина «кибербезопасность» положены также результаты сравнительного анализа функционального соотношения (парадигмы) понятий «кибербезопасность» и «информационная безопасность» с учетом необходимого соответствия паритету в информационном противоборстве. Сформированы некоторые предложения по реализации и развитию кибербезопасности в Российской Федерации.*

***Ключевые слова:*** *облачные вычисления, интернет вещей, виртуализация, киберпространство, инфосфера, информационная безопасность, функциональная устойчивость, информационное противоборство, мониторинг, компьютерная атака, криптоподсистема, система защиты информации, парадигма, eSIM технологии.*

**DOI:**10.21681/2311-3456-2021-4-61-72

## Введение

Следует отметить, что термин «кибербезопасность» появился и нашел свое применение в ведущих развитых странах мира в конце 90-х начале 2000-х лет. В последующем он нашел свое признание и применение в среде международного общения в части разработки и подписания в области международной безопасности некоторых международных стандартов, деклараций, обращений и других документов. Однако в действующем российском законодательстве даже в 2015 году его еще не было [1], и разработчики не могли прийти к единому мнению по его определению и применению.

Ведущие зарубежные страны увидели в нем новую содержательную сущность в области национальной и международной безопасности, предали ему важное значение, разработали и сформировали его раскрытие и понятийный аппарат для обеспечения однозначного взаимопонимания и общения.

С учетом этого, признавая исключительное значение национальной безопасности, большинство ведущих зарубежных стран разработали и ввели в действие ряд основополагающих доктринальных документов национальной безопасности таких как: Концепция, Стратегия и Политика кибербезопасности и др. более частных.

Аналогичная работа велась и ведется в настоящее время и в области международной безопасности.

В Российской Федерации признание и применение термина «кибербезопасность» имело и имеет до сих пор проблематичный характер от абсолютного его отрицания, до некоторого, начиная с 2016–2017 гг., корпоративного использования.

И особенно эта проблематичность и противостояние связаны с позицией наших регуляторов в области информационной безопасности, которые обеспокоены неаргументированным предположением о том, что признание и применение термина приведут к необходимости революционного изменения нормативно-методического регулирования и создания базы новых национальных стандартов. Однако, чтобы понять этот объем «бедствий» необходимо разобраться, а что это такое, что нового это вносит в область информационной безопасности. В каком сущностном соотношении находятся «кибербезопасность» и «информационная безопасность» в предметной и функциональной областях.

После этого, важно оценить в каком состоянии находится реализация и развитие кибербезопасности в Российской Федерации. Какие научно-технические проблемы реализации и развития существуют на сегодняшний день. Важно определить и сформулировать предложения по их разрешению.

1 Добродеев Александр Юрьевич, кандидат технических наук, старший научный сотрудник, советник генерального директора ФГУП «Центральный научно-исследовательский институт связи», г. Москва, Россия. E-mail: a.dobrodeev@zniis.ru

Еще 26 февраля 2013 г. на совещании в Совете Федерации РФ «О разработке стратегии национальной кибербезопасности Российской Федерации: состояния, предпосылки, механизмы и перспективы» член Комитета Совета Федерации по науке, образованию, культуре и информационной политике, председатель временной Комиссии Совета Федерации по развитию информационного общества Руслан Гаттаров провозгласил: «Кибербезопасность» было непонятным, почти ругательным словом, теперь это – насущная проблема, а мы – на пути её решения» [2].

Дискуссионную попытку разобраться в этих вопросах и предлагает эта статья.

### 1. Значение, роль и место кибербезопасности в национальной и международной безопасности XXI века

Современный этап мирового и национального развития характеризуется тем, что кибербезопасность закономерно занимает лидирующие позиции в процессе обеспечения национальной и международной безопасности XXI века.

Информационное противоборство в современном мире уже приобрело и всё более приобретает постоянно действующий, активный, изощрённый и развивающийся характер информационной войны за гегемонию и мировое господство [3, 11].

Стремительное развитие информационных технологий, широкая информатизация всех сторон жизни общества и вооруженных сил ведущих зарубежных государств значительно изменили характер и методы деятельности государственных, правительственных политических и экономических структур, оказали влияние на социальные взаимосвязи, сформировали новые информационные угрозы и вызовы, в том числе и в киберпространстве [4].

Еще в начале XXI века в ряде зарубежных концептуальных и нормативно-правовых документов устоялись такие термины, как «кибер-война» (cyber war), «боевые действия в киберпространстве» (cyber warfare), «кибератака» (cyber attack) и ряд других схожих с ними, содержательная часть которых подразумевает противоборство и решение боевых задач в киберпространстве (cyberspace) [5].

Военное и политическое руководство США рассматривает безопасность в кибернетическом пространстве (кибербезопасность) в качестве одного из ключевых факторов обеспечения национальной безопасности государства [6].

Так, например, Пентагон признал киберпространство новым полем возможных боевых действий, а НАТО утвердило приравнивание кибератак к вооружённому нападению. В «Международной стратегии США для киберпространства» (2011г.) акты компьютерных диверсий приравнены к традиционным военным действиям с правом реагировать на них всеми средствами, вплоть до применения ядерного оружия.

Согласно документу[2], под «кибернетическим пространством» («киберпространством») понимается глобальная инфраструктура, состоящая из взаимосвязанных информационных структур, в том числе глобальной компьютерной сети Интернет, телекоммуникационных сетей, вычислительных систем, процессоров и контроллеров, встроенных в технические средства, а также из персонала, использующего их в своей деятельности или обеспечивающего их функционирование.

Военно-политическим руководством ведущих государств мира противоборство в киберпространстве по-прежнему рассматривается как одно из решающих условий реализации национальных интересов и выгодного урегулирования кризисных ситуаций. С учетом решения этой задачи развиваются национальные и межгосударственные органы управления, силы и средства кибервойн, реализуются новые подходы к построению системы противоборства в киберпространстве на всех уровнях.

***Таким образам, киберпространство становится неразрывной частью сферы ведения военных действий, особенно в том случае, если системы управления сторон конфликта строятся по сетецентрическому принципу. Войны в киберпространстве являются новой разновидностью противоборства, которая в перспективе может оказать решающее влияние на ход и исход военных действий. В настоящее время существует развитый арсенал средств, для проведения кибероперaций, от которых достаточно сложно защититься [5,7] .***

Кроме того, зависимость безопасности и экономики страны от состояния важных объектов и систем инфраструктуры (энергообеспечения, водоснабжения, вычислительных сетей, телекоммуникации и связи, транспорта и др.) на фоне возможного скрытного информационно — технического воздействия на них с целью нарушения работоспособности или прекращения функционирования вынуждает американские власти уделять первоочередное внимание проблемам обеспечения информационной безопасности (киберзащиты) автоматизированных систем управления и информационных ресурсов объектов национальной инфраструктуры [6].

Согласно официальным данным, наибольшему количеству кибернетических атак подвергаются организации и предприятия энергетического, финансового, промышленного и транспортного секторов инфраструктуры, а также информационные ресурсы министерств и ведомств (государственно-управленческого сектора инфраструктуры) США. Более того, в последнее время отмечается возрастание опасности такого явления, как кибертерроризм. Действия по дезорганизации информационных систем, создающие опасность гибели людей, значительного имущественного ущерба или иных общественно опасных последствий, совершаемых с целью нарушения общественной безопасности, устрашения населения путем создания условий для аварий и катастроф техногенного характера либо оказания

2 Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms. 8 November 2010 (As Amended Through 15 November 2011)

воздействия на органы власти с целью принятия ими решений, необходимых террористам, в том числе провоцирующих военные конфликты. Наряду с кибертерроризмом американские эксперты выделяют ряд аспектов проблемы кибербезопасности: киберпреступность, кибервойну и отдельно – управление глобальной сетью Интернет [6].

Таким образом, перспективы решения задачи киберзащиты инфраструктуры США военное и политическое руководство страны связывает с необходимостью концентрации усилий на предотвращении кибератак против национальных объектов [6].

### 2.Состояние и пути развития кибербезопасности ведущих зарубежных стран

Общим однозначным выводом является то, что в современных и перспективных условиях информационного противоборства кибербезопасность приобретает чрезвычайно важное базовое значение в части обеспечения безопасности личности, общества и государства в целом, она является основой национальной и международной безопасности XXI века.

На примере США нетрудно показать какое значение придается кибербезопасности (киберзащите) в обеспечении национальной безопасности государства.

Так, в принятой в США еще в 2003 году «Национальной стратегии кибербезопасности» термин «кибербезопасность» употреблялся для обобщения всей деятельности, связанной с защитой информации и информационных ресурсов [4].

В документе подчеркивалось, что обеспечение кибербезопасности является «важнейшей стратегической задачей, решение которой требует скоординированных и целенаправленных усилий всего общества, федерального правительства, органов власти штатов и территориальных административных образований, бизнеса и всего американского народа». Особо отмечалось, что обеспечение кибербезопасности призвано укрепить национальную систему безопасности и важная роль в решении этой задачи отводится вооруженным силам [4].

Дальнейшее отражение вопросы противоборства в киберпространстве нашли в «Национальной военной стратегии США» 2004 года, определившей киберпространство как «сферу ведения боевых действий наряду с наземной, морской и воздушно-космической сферами», а также в принятой в 2006 году «Национальной военной стратегии в области кибероперациий», установившей новую форму действий ВС — операции в киберпространстве [4,6].

Кроме того, в 2004 году руководством США принят «Национальный план реагирования» с приложением посвященном кибербезопасности (киберзащите), а в 2009 году принят подготовленный МО США «План защиты национальной инфраструктуры», на основании которого сформирована Концепция защиты киберпространства США, аналогичное концепции защиты критической инфраструктуры.

В дальнейшем вопросы противоборства в киберпространстве были закреплены и раскрыты в «Национальной военной стратегии США» 2011 года и утвержденной в том же году «Стратегии действий министерства обороны США в киберпространстве». Были уточнены директивы министра обороны, руководства и наставления объединенного комитета начальников штабов, уставы и другие руководящие документы видов ВС, сформированы соответствующие киберкомандования, подготовлены силы и средства ведения указанных операций.

Официально киберкомандование приступило к работе в мае 2010 года в составе объединенного стратегического командования (ОСК) и, по мнению руководства страны, достигло полной оперативной готовности спустя шесть месяцев — в конце октября. Оно объединило под своим началом несколько ранее существовавших организаций, в частности оперативно-тактическую группу сетевых операций (JTF-GNO) и командование боевых действий в информационных сетях (JFCC-NW). Управление информационных систем МО США было переведено в штаб-квартиру киберкомандования в Форт-Мид (штат Мэриленд) [4].

Согласно действующей стратегии страны по обеспечению безопасности киберпространства, требуется дальнейшее расширение возможностей киберразведки и национальной системы киберзащиты для превентивных кибердаров и заблаговременного проникновения в информационные системы противника до момента начала его кибератаки.

В идеале система киберзащиты США должна быть нацелена на реализацию возможности нанесения превентивных кибердаров, а также проникновения в информационные системы противника до начала им кибератаки.

Для эффективного решения задач обеспечения кибербезопасности (киберзащиты) в интересах национальной безопасности в США разработана стратегия «единства усилий», в рамках которой для решения этих задач объединены усилия всех важных министерств, ведомств, силовых структур и ведущих коммерческих организаций [6].

Ответственность за эффективное решение задач кибербезопасности возложена на Управление национальной безопасности (УНБ) и Министерство внутренней безопасности (МВБ), в рамках которого созданы и функционируют такие структурные подразделения как:

— Центр МВБ по киберзащите;
— Управление кибербезопасности и коммуникаций МВБ, в составе которого функционируют:
— национальное подразделение кибербезопасности с командным пунктом киберзащиты;
— центр экстренного реагирования на компьютерные происшествия с группами экстренного реагирования.

Все это еще раз подчеркивает стратегическое отношение США к вопросам создания и применения системы обеспечения кибербезопасности страны в интересах ее национальной безопасности [6].

Аналогичные серьезные меры в отношении кибербезопасности предприняты большинством ведущих стран мира, таких как: Великобритания, Германия, Франция, Китай, Корея и др.

В настоящее время более чем в 40 ведущих стран мира разработаны и приняты такие базовые документы как Концепция и/или Стратегия кибербезопасности,

DOI:10.21681/2311-3456-2021-4-61-72

а также наиболее важные решения и меры в части кибербезопасности перенесены и приняты военно-политическим альянсом НАТО.

В силовых структурах ряда зарубежных стран созданы и развиваются соответствующие командования и структуры, создаются и совершенствуются силы и средства противоборства в киберпространстве.

Появились и стали быстро распространяться и развиваться средства ведения противоборства в киберпространстве, так называемое кибероружие. Ущерб от его использования может приводить к техногенным катастрофам на критически важных объектах промышленности, экономики, энергетики и транспорта, к финансовому коллапсу и системному экономическому кризису. Задействование такого боевого средства способно существенно дезорганизовать государственное и военное управление, деморализовать и дезориентировать население, создать массовую панику и хаос.

Ситуацию обостряет тот факт, что разработка и создание образцов кибероружия обходятся значительно дешевле, чем иных видов оружия, применение которых приводит к аналогичному ущербу. В настоящее время этим занимаются в более чем 120 странах, межгосударственных объединениях, организациях и сообществах хакеров, в то время как разработкой ядерного оружия — максимум в 20 [5].

И стратегия НАТО стала еще одним шагом на пути создания систем глобального контроля киберпространства, но теперь уже при поддержке всего спектра военных возможностей и с учетом вероятных попыток взлома военных информационных систем со стороны других государств и хакерских групп.

Военно-политическое руководство ведущих зарубежных государств признает, что успешная организация и ведение противоборства в киберпространстве обеспечивают благоприятные условия для эффективного ведения военных операций в других сферах вооруженного противостояния (на суше, на море, в воздухе и в космосе) и любом географическом регионе мира. При этом особое значение придается завоеванию превосходства в киберпространстве (cyberspace superiority). Под данным термином понимается «оперативное преимущество, полученное в самом киберпространстве или путем его использования, позволяющее проводить операции в установленные сроки и в конкретной области без внешних препятствий этому» [4].

Превосходство в киберпространстве достигается решением трех взаимосвязанных задач [4]:

— обеспечение функционирования киберпространства (cyberspace support);
— оборона киберпространства (cyberspace defense);
— применение киберсил (cyberspace force application).

Задача обеспечения функционирования киберпространства предполагает построение, развертывание и обеспечение надежной работы глобальной информационной сети (сеть министерства обороны США), включая вопросы безопасности, контроля соблюдения правил работы в сети и обеспечения информационной гарантии (доступности, целостности, аутентификации и конфиденциальности информации).

По мнению военно-политического руководства ведущих зарубежных государств, задача обороны своего киберпространства охватывает весь набор мер пассивной и активной киберзащиты от существующих или потенциальных угроз, включая в определенных условиях воздействие на источники таких угроз за пределами своих сетей. В рамках этой задачи также решается ряд вопросов обеспечения информационной безопасности.

Задача применения киберсил предполагает применение специальных сил и средств, позволяющих вести активные действия в самом киберпространстве в интересах достижения военных целей и влияния на развитие ситуации в нужном направлении. Такие действия одновременно нацелены на глубокое проникновение и обеспечение доступности к ресурсам мирового информационного пространства.

В рамках всех трех задач решаются также вопросы разведывательно-информационного обеспечения операций, поддержки информационных операций, обеспечения боевого управления, гарантии выполнения боевой задачи (достижение основных целей боевой задачи) и ситуационной осведомленности. Последнее означает предоставление и постоянное обновление данных об обстановке, в том числе в визуальной форме.

Формирование в единый образ обстановки фрагментов боевого пространства, получаемых по различным каналам связи и передачи информации, отражает суть режима ситуационной осведомленности.

Каждая задача подразумевает проведение определенного набора действий, которые, по существу, и формируют спектр операций в киберпространстве (cyberspace operations). Под ними понимается «применение кибернетических средств в целях выполнения военных задач и достижения необходимых результатов как в самом киберпространстве, так и с его использованием».

***Таким образом, обобщая взгляды военно-политического руководства ведущих зарубежных государств и содержание материалов соответствующих доктринальных документов, рассматривая структуру органов, планы по развитию сил и средств, ответственных за организацию и ведение противоборства в киберпространстве, можно сделать вывод, что одной из перспективных форм применения вооруженных сил в современных условиях становится проведение операций в киберпространстве. Большинство ведущих зарубежных государств имеют и реализуют программы и планы как по обеспечению кибербезопасности, так и по подготовке ВС к организации и проведению таких операций [4].***

### 3. Проблемные вопросы реализации и развития кибербезопасности в Российской Федерации

Проблемы реализации и развития кибербезопасности в России, на наш взгляд, связаны с тремя принципиальными основными причинами:

— с неоднозначным толкованием термина и понятия «кибербезопасность» в связи с отсутствием корректного их раскрытия и принятия;

— с отсутствием и невозможностью учета в современной системе защиты информации, реализующей лишь оборонительные функции, особенностей современного этапа информационного противоборства, требующего создания и применения сил и средств превентивного противодействия опасным информационным силам и средствам противоборствующей стороны;
— с отсутствием результатов корректного соотношения (парадигмы) терминов и понятий «информационная безопасность» и «кибербезопасность» уточняющих достаточность и возможности использования существующих нормативно-методических документов и национальных стандартов в области информационной безопасности и уточняющих необходимость их корректировки и разработки новых.

Эффективное решение задач обеспечения кибербезопасности государства, общества и личности невозможно без однозначного понимания её содержательной сущности и раскрытия понятийного аппарата в этой области [5,7,8].

Признание и принятие самого термина кибербезопасность у нас в стране до 2016 года было весьма сложным и проблематичным.

Одной из причин непринятия ранее этого термина в нашей стране являлось необоснованная констатация абсолютного соответствия терминов «информационная безопасность» и «кибербезопасность» (либо их противопоставление). Отрицание его введения обосновывалось опасением необходимости разработки новой нормативно-методической базы и новых национальных стандартов в части кибербезопасности. Детального сравнительного анализа содержательного соотношения между этими терминами не проводилось. Неизвестно и о попытках раскрытия и сравнения этих терминов в области понятийного аппарата.

И если ранее необходимость его признания в России определялась необходимостью взаимопонимания и паритета на международном уровне общения и подписания международных документов, то в настоящее время, после включения «Технологий кибербезопасности» Распоряжением Правительства Российской Федерации 2016 г. в Перечень приоритетных технологических направлений ОПК РФ (на основании Указа Президента РФ от 20 июля 2016 года № 347) его признание в стране приняло конкретное практическое значение [10].

Поэтому после законодательного введения термина «кибербезопасность» возникла необходимость уточнения его содержательной сущности и понятийного аппарата, что позволит корректно построить исследования и разработки в областях информационной безопасности и кибербезопасности.

К сожалению, до настоящего времени раскрытие термина «кибербезопасность», его определение и понятие на законодательно – правовом уровне в Российской Федерации не произведено. Известны лишь попытки дискуссионного обсуждения этой проблематики на форумах, конференциях и в публикациях в научно – технических журналах и, как пример, на страницах журнала «Вопросы кибербезопасности» [8].

Сложившаяся ситуация создаёт серьезные трудности во взаимопонимании, в формировании программ и задач исследований и разработок, в необходимости создания в этой области новой нормативно – методической базы – национальных стандартов, а также в законном использовании уже имеющейся базы этих документов для области информационной безопасности и защиты информации.

В большинстве случаев даже в научной среде исследователями и разработчиками продолжаются попытки противопоставить по сущности кибербезопасность и информационную безопасность, не рассматривая соотношения между ними.

Следует констатировать крайнюю необходимость в наведении строгого порядка в понятийном аппарате и правильном содержательном использовании этой терминологии на основе уточнения требуемых функциональных возможностей и предметной области исследований, разработок и особенностей применения.

При этом необходимо использовать зарубежный опыт в формировании проблематики кибербезопасности, поскольку за рубежом этот термин и его понятие были приняты и раскрыты уже на рубеже 2000 года в порядке разработок таких стратегических национальных и международных документов как политика, стратегия и концепция кибербезопасности. В международном сообществе в этой проблематике заняты и работают более 40 стран.

Поэтому разработку отечественного понятийного аппарата в области кибербезопасности следует делать с учётом зарубежного опыта в том числе и в части понятийного аппарата, и в части реализации функциональных возможностей.

За рубежом разработка понятийного аппарата начата с формирования понятия киберпространство, с предметной области (сферы) обеспечения (реализации) кибербезопасности, содержательная сущность которого раскрывается следующим образом.

### 4. Варианты раскрытия термина «киберпространство»

#### А. Международная политическая трактовка понятия киберпространство

**Киберпространство** – как новая сфера (среда) противоборства конкурирующих государств. Пентагон признал киберпространство новым полем возможных боевых действий, а НАТО утвердило приравнивание кибератак к вооружённому нападению.

В «Международной стратегии США для киберпространства» (2011г.) акты компьютерных диверсий приравнены к традиционным военным действиям с правом реагировать на них всеми средствами, вплоть до применения ядерного оружия.

#### Б. Техническая трактовка понятия киберпространство.

1. **Киберпространство** – глобальная сфера (область, домен) внутри информационного пространства,

представляющего собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая интернет, телекоммуникационные сети, компьютерные системы, а также встроенные в другие технические объекты процессоры и контроллеры, предназначенные для хранения, обработки, модификации и обмена данными. (Операции в киберпространстве, МО США, 2010г., Единый устав КНШ США, 2001г.) [6,7].

2. **Киберпространство** – пространство, сформированное за счёт функционального объединения взаимосвязанных сетей компьютеров, информационных сетей и телекоммуникационных инфраструктур в целом трактуемая как WorldWideWeb. («Законы информационного конфликта: Законы в сфере безопасности национального киберпространства», Томас Вингфилд, 2000г.).

Поэтому в краткой зарубежной трактовке под кибербезопасностью понимается информационная безопасность в киберпространстве.

В российской интерпретации трактовку термина и понятия «Киберпространство» удобно произвести, используя сущностное понятие и термин инфосфера (информационная сфера), раскрытых в «Доктрине информационной безопасности Российской Федерации» (2016г) и в ГОСТ Р 51583 – 2000, которые формулируются следующим образом:

1. Информационная сфера (Инфосфера) – это совокупность информации, объектов информации, информационные системы, сайтов информационно – телекоммуникационной сети “Интернет”, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и оборотом информации, развитием и использованием названных технологий, обеспечением информационной безопасности (Указ Президента РФ от 5 декабря 2016г. № 646.Об утверждении «Доктрины информационной безопасности Российской Федерации»).
2. Информационная сфера (Инфосфера) – это сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации (ГОСТ Р 51583 – 2000. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении).

Таким образом в соответствии с изложенным, сферой реализации (обеспечения) кибербезопасности является компьютерно – телекоммуникационная инфосфера или, в иностранной трактовке, – киберпространство.

Компьютерно – телекоммуникационную инфосферу предлагается определить как: совокупность компьютерных информационно – управляющих вычислительных и телекоммуникационных инфраструктур и средств, в том числе контроллеров, процессоров и т.д. в субъектах информатизации и в настоящее время «интернет вещей».

Легко удостовериться при этом в большом сходстве этой формулировки с раскрытой технической трактовкой иностранного термина «киберпространство».

Таким образом, с учётом уточнения предметной области реализации (обеспечения) термин «кибербезопасность» по сути может быть раскрыт следующими определениями [10 ].

### 5. Некоторые варианты раскрытия термина и понятия «кибербезопасность»

**А. Через раскрытие термина с учетом перевода с английского**

**Кибербезопасность:** это информационная безопасность в сфере (области) информационных технологий , компьютерных технологий и управления.

**Б. Через техническую трактовку понятия киберпространство**

**Кибербезопасность:** это информационная безопасность в киберпространстве.

**В. Через увязку с целями информационной безопасности, определёнными «Доктриной информационной безопасности Российской Федерации»**

(обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры и единой сети электросвязи РФ в мирное время, в период непосредственной угрозы агрессии и в военное время).

**Кибербезопасность:** это свойство (состояние) компьютерных информационно – управляющих и телекоммуникационных инфраструктур сохранять заданную функциональную устойчивость при гарантированном соответствии требованиям информационной безопасности.

**Г. Через соотношение понятий информационная безопасность и кибербезопасность**

**Кибербезопасность:** это информационная безопасность в инфосфере компьютерных информационно – управляющих и телекоммуникационных инфраструктур.

**Кибербезопасность:** это информационная безопасность в компьютерно-инфотелекоммуникационной инфосфере.

**Таким образом, общее определение может выглядеть так:**

**Кибербезопасность: это свойство (состояние) сохранять заданную функциональную устойчивость при гарантированном соответствии требованиям информационной безопасности (защиты информации) в современных и перспективных условиях информационного противоборства.**

Нетрудно заметить, что предлагаемые формулировки термина «кибербезопасность» не противоречат друг другу, а лишь дополняют и уточняют смысловое содержание.

В них уточнено современное видение функциональной достаточности кибербезопасности и путей её достижения и развития в части разработки и совершенствования средств и технологий информационной безопасности.

В современных и перспективных условиях совершенствования методов и средств информационного противоборства, постоянного выявления новых уязвимостей и угроз, развития и изощрённого применения компьютерных атак, требования к кибербезопасности постоянно растут, в том числе и в части расширения

методов и средств защиты и информационного противоборства.

В соответствии с этим в настоящее время кибербезопасность должна обеспечивать не только заданную функциональную устойчивость при гарантированном соответствии требованиям информационной безопасности, но и реализовывать мониторинг и отражение компьютерных атак, а также реализовывать информационное противодействие противнику.

Таким образом базовая современная модель кибербезопасности должна содержать в своём составе не только классическую систему защиты от НСД, криптоподсистему, систему обнаружения вторжений и/или систему обнаружения, предупреждения и ликвидации последствий компьютерных атак («ГОСсопка»), но и, при необходимости, модули и механизмы отвлечения противника на ложные цели, а также средства отражения информационных атак и противодействия им, превентивного отражения опасных информационных сил и средств противоборствующей стороны в угрожаемый период и военное время [10 ].

Однако и эти формулировки, раскрывающие сущность термина и понятия «кибербезопасность», не следует считать полнодостаточными или окончательными.

Следует обязательно учесть особенности современного этапа информационного противоборства, оценить необходимые меры и средства, в том числе, паритетного противодействия и противоборства и на основании этого определить соотношение (парадигму) понятий «информационная безопасность» «кибербезопасность». На наш взгляд эти особенности и связанными с ними результаты и позволяют уточнить формулировки раскрытия термина и понятия «кибербезопасность».

В этой части некоторые общие результаты и выводы сформулированы ранее в работах [8, 9, 10, 12]. Там же приведена обобщенная структурно-функциональная схема обеспечения и реализации кибербезопасности объектов информатизации.

Проведенный выше анализ позволяет представить обобщенную схему соотношения (парадигмы) понятий «информационная безопасность» и «кибербезопасность» как показано на рисунке ниже.

С учетом этого и вытекают более развернутые формулировки (определения) термина и понятия «кибербезопасность» в следующем виде.

**Кибербезопасность** – это информационная безопасность компьютерной и инфотелекоммуникационной инфосферы (в том числе в части процессов, контроллеров и «интернет вещей») в современных условиях информационного противоборства, реализующая дополнительно в системе защиты информации не только оборонительные функции, но и функции привентивного воздействия и подавления враждебных и опасных информационных сил и средств противника в угрожаемый период и в военное время.

С учетом того, что кибербезопасность фактически это состояние или свойство объекта информатизации (изделия, комплекса, системы информатизации) опре-

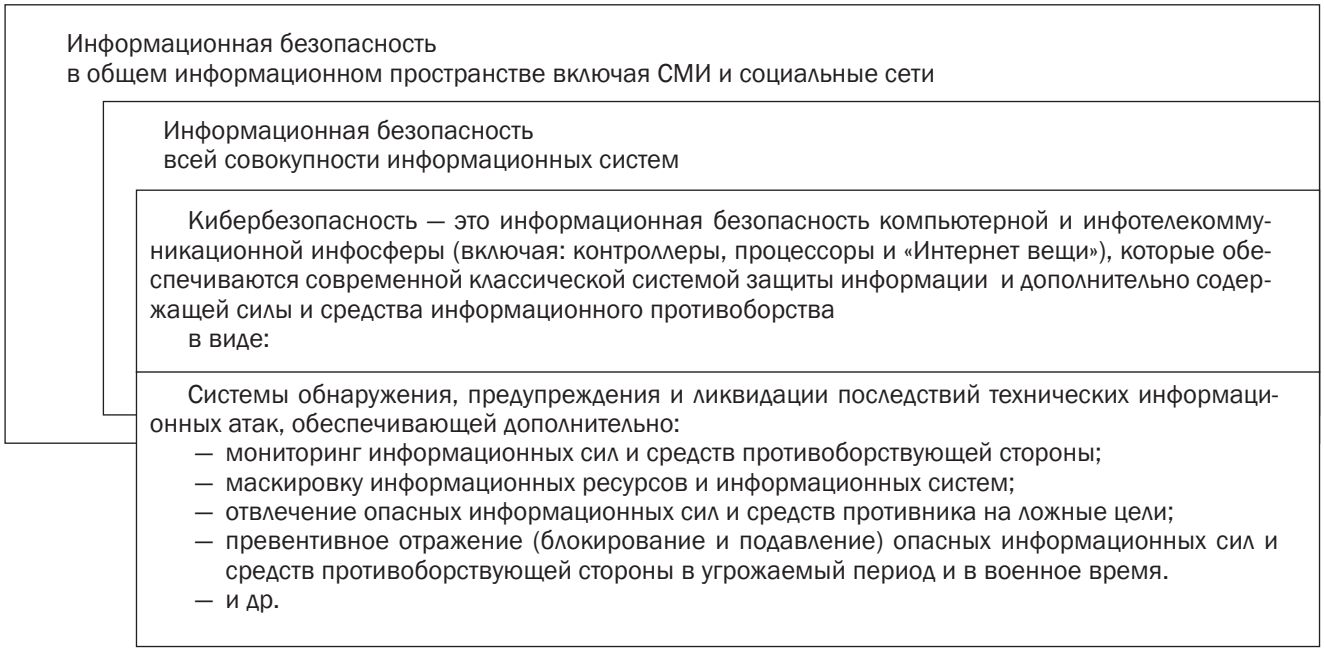


*Рис.1 Предлагаемая схема соотношения (парадигмы) понятий «информационная безопасность» и «кибербезопасность»*

Таким образом, «кибербезопасность» в термине «информационная безопасность» должна неукоснительно содержать не только оборонительные, но и превентивные функции относительно опасных информационных сил и средств противоборствующей стороны.

DOI:10.21681/2311-3456-2021-4-61-72

деление этого термина может быть раскрыто следующим образом:

**Кибербезопасность** – это свойство (состояние) объекта информатизации (изделия, комплекса, системы информатизации) сохранять заданную функциональную устойчивость (штатное функционирование) в части гарантий обеспечения информационной безопасности с возможностью превентивного противодействия опасным информационным силам и средствам противника в условиях современного и перспективного информационного противоборства.

Не трудно заметить, что раскрытия этих определений тоже не противоречат, а дополняют друг друга.

Важным выводом анализа содержательной сущности раскрытых формулировок термина «кибербезопасность» является то, что они устраняют многие кажущиеся противоречия с сутью термина «информационная безопасность», определяя, как важную предметную область в ней. Отсюда следует лишь некоторая необходимость разработки принципиально новой нормативно – методической документации и национальных стандартов в области кибербезопасности, поскольку на неё в полном объёме распространяется актуальная документация области информационной безопасности.

Безусловно требуются некоторые доработки, уточнения и разработки дополнительных документов в части динамики появления новых уязвимостей и угроз и реализации (при необходимости) новых возможностей и механизмов обеспечения кибербезопасности. Плановая работа в этой области в части разработки национальных стандартов ведётся в стране техническими комитетами ТК – 26, ТК – 362 и ТК – 194.

### 6. Состояние и пути развития кибербезопасности и технологий кибербезопасности в Российской Федерации

Объективно и в России обеспечение кибербезопасности на государственном – национальном уровне приобретает всё возрастающее значение и актуальность.

Этим объясняются решительные действия руководства нашей страны в части реализации мер обеспечения кибербезопасности государства созданием института приоритетных технологических направлений, одним из важнейших в котором является приоритетное технологическое направление «Технологии кибербезопасности».

Впервые в Российской Федерации приоритетные направления развития технологий определены в Указе Президента РФ от 7 июля 2011 года № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации» с внесенными изменениями и дополнениями Указом Президента РФ от 16 декабря 2015 года № 623.

Начиная с 2016 года по настоящее время в Российской Федерации в целях создания и реализации единой промышленной и научно-технической политики развития инновационных технологий в ОПК и разработки новых (перспективных) образцов (комплексов, систем) вооружения военной и специальной техники (ВВСТ) законодательно-правовыми и руководящими документами РФ формируется и вводится в действие институт (орган) приоритетных технологических направлений (ПТН) [10 ].

Базовый перечень законодательно — правовых документов, определяющих создание и деятельность института приоритетных технологических направлений России представлен в Таблице ниже.

Основными задачами института ПТН, вытекающими из этого базового перечня, являются:

1. Формирование и реализация единой промышленной и научно-технической политики развития инновационных технологий в ОПК РФ и разработки образцов ВВСТ.
2. Разработка и представление в установленном порядке предложений по постановке и выполнению научно-исследовательских, опытно-конструкторских и технологических работ, направленных на создание и внедрение промышленных технологий для инновационного развития ОПК РФ и обеспечения высокого технического уровня ВВСТ.
3. Разработка предложений по постановке и организация выполнения и сопровождения НИР, ОКР и технологических работ, необходимых для создания научно-технического задела.
4. Разработка Комплексных целевых программ развития приоритетного технологического направления и планов их реализации.
5. Разработка и представление на обсуждение в НТС ВПК РФ предложений по проектам перечней новых базовых и критических промышленных технологий, входящих в состав единой системы исходных данных для программно-целевого обеспечения реализации военно-технической политики Российской Федерации.
6. Периодическое проведение анализа современных промышленных технологий в стране и за рубежом в области ПТН с целью разработки перспективных инновационных промышленных технологий в интересах создания ВВСТ.
7. Осуществление мониторинга достижений ведущих иностранных государств в области науки, техники и технологий, с ежегодным предоставлением соответствующего аналитического отчета и предложений в НТС ВПК РФ.
8. Периодическое проведение анализа научных и производственных возможностей ОПК РФ и других ведущих организаций страны в области ПТН и на его основе разработка предложений по формированию рациональной кооперации исполнителей создания современных образцов и систем ВВСТ.
9. Координация работ, выполняемых в рамках ПТН, их увязка с технологическими работами, фундаментальными, поисковыми и прогнозными исследованиями, проводимыми в ходе реализации государственных, федеральных и иных программ в сфере обеспечения обороны страны и безопасности государства.
10. Осуществление научно-технического сопровождения работ, выполняемых организациями, участвующими в реализации ПТН.

*Таблица 1*

*Базовые законодательно-правовые документы, определяющие создание и деятельность института приоритетных технологических направлений России*

**Цель создания института приоритетных технологических направлений** — создание и реализация единой промышленной и научно-технической политики в стране по развитию инновационных технологий в ОПК для разработки новых (перспективных) образцов (комплексов, систем) вооружения, военной и специальной техники (ВВСТ) обороны Российской Федерации.

| |
|---|
| Указ Президента РФ от 07.07.2011 г. № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации» и Указ Президента РФ от 16.12.2015 г. №623 «О внесении изменений и дополнений...» |

| | | |
|---|---|---|
| Указ Президента Российской Федерации от 20 июля 2016 года №347 «О руководителях приоритетного технологического направления». Утверждено «Положение о руководителе приоритетного технологического направления». | Постановление правительства РФ от 10 сентября 2016 года № 944. Об утверждении «Правил включения организаций оборонно-промышленного комплекса в перечень приоритетных технологических направлений, организаций ОПК, осуществляющих научную (научно-исследовательскую) деятельность и ответственных за их реализацию». | Протокол заседания НТС ВПК РФ от 1 августа 2017 года № ВПК(НТС)-28(109) пр. О проекте «Порядка взаимодействия руководителя ПТН с федеральными органами исполнительной власти, организациями, участвующими в реализации приоритетного технологического направления, другими организациями и генеральными конструкторами по созданию ВВСТ». |

| |
|---|
| Протоколы заседаний ВПК и коллегий ВПК, Решений и Распоряжений правительства Российской Федерации в 2016-2017 гг. определили Перечень ПТН и организаций ОПК РФ, осуществляющих научную (научно-исследовательскую) деятельность и ответственных за их реализацию и полномочных руководителей ПТН по каждому направлению. Утвердили порядок взаимодействия руководителей ПТН с ФОИВ, с организациями, участвующими в реализации ПТН (в том числе с ФПИ), с другими организациями и Генеральными конструкторами по созданию ВВСТ. |

11. Координация деятельности организаций в части реализации ПТН, в том числе во взаимодействии с Генеральными конструкторами по разработкам ВВСТ.
12. Разработка рекомендаций по технологическому обеспечению развития систем вооружения и оборонно-промышленного комплекса Российской Федерации.
13. Разработка предложений по уточнению действующих и разработке новых национальных, государственных и отраслевых стандартов в области реализации ПТН.

В настоящее время процесс формирования и становления института руководителей ПТН находится на завершающей стадии с уточнением порядка работы и взаимодействия его с Федеральными органами исполнительной власти (ФОИВ), министерствами, ведомствами и ведущими предприятиями в этой области исследований и разработок.

Началом создания института руководителей ПТН является Указ Президента РФ «О руководителе приоритетного технологического направления» № 347 от 20 июля 2016 года, которым утверждено Положение о руководителе приоритетного технологического направления.

Утвержденное Положение определяет права, обязанности и ответственность руководителя ПТН и регулирует другие вопросы, связанные с его деятельностью.

Положение также определяет порядок формирования Перечня приоритетных технологических направлений на основе приоритетных направлений развития науки, технологий и техники РФ и Перечня критических технологий РФ, утвержденных Президентом РФ. Перечень ПТН определяет Правительство РФ по представлению коллегии ВПК РФ.

«Правила включения организаций оборонно-промышленного комплекса в перечень приоритетных технологических направлений, организаций оборонно-промышленного комплекса, осуществляющих научную (научно-исследовательскую) деятельность и ответственных за их реализацию» утверждены Постановлением правительства РФ от 10 сентября 2016 года № 944.

Последующими документами руководства страны и ее органов (Таблица 1) в 2016-2017 гг. определены: Перечень приоритетных технологических направлений, организаций ОПК, осуществляющих научную (научно-исследовательскую) деятельность и ответственных за их

DOI:10.21681/2311-3456-2021-4-61-72

реализацию, полномочные руководители ПТН по каждому направлению, утвержден порядок взаимодействия руководителей ПТН с ФОИВ, с организациями, участвующими в реализации ПТН (в том числе с Фондом перспективных исследований), с другими организациями и Генеральными конструкторами по созданию ВВСТ.

В соответствии с утвержденным Перечнем ПТН за реализацию ПТН «Технологии кибербезопасности» поручено отвечать АО «Концерн «Автоматика» [10].

Перечень приоритетных технологических направлений, организаций оборонно-промышленного комплекса, осуществляющих научную (научно-исследовательскую) деятельность и ответственных за их реализацию представлен коллегией ВПК РФ и утвержден Распоряжением Правительства Российской Федерации в 2016 году.

В соответствии с протокольными решениями заседаний НТС ВПК РФ руководителями ПТН разработаны и утверждены в НТС ВПК РФ базовые нормативно-технических документы, в составе:

— перечень разделов приоритетного технологического направления и пути
— их развития;
— перечень базовых и критических промышленных технологий по направлению;
— комплексные целевые программы развития приоритетного технологического направления и планы мероприятий по их реализации.

Перечни разделов ПТН и базовых и критических промышленных технологий определяют тематику и основные направления фундаментально – поисковых и прикладных исследований и разработок в интересах создания современных ВВСТ обороны государства [10].

Согласованные и утвержденные комплексные целевые программы приоритетных технологических направлений предназначены для создания базовой основы разработки и корректировки государственных программ исследований и разработок в областях ПТН, в том числе в области ПТН «Технологии кибербезопасности».

### 7. Некоторые предложения по реализации и развитию кибербезопасности в Российской Федерации

С учетом изложенного, следует отметить, что реализация и развитие кибербезопасности в Российской Федерации в настоящее время в сильной мере зависит от двух основополагающих факторов, к которым следует отнести:

— совершенствование и повышение эффективности практической деятельности приоритетного технологического направления «Технологии кибербезопасности» в лице организации отвечающей за его реализацию;
— скорейшее наведение порядка и создание стройной системы нормативно-методического регулирования и разработка необходимых национальных стандартов в этой области.

Последнее может быть успешно разрешено по инициативе ПТН «Технологии кибербезопасности» техническими комитетами ТК-26, ТК-362 и ТК-194 (в отдельных случаях возможно их объединенными усилиями).

Следует полагать, что начать эту работу необходимо с разработки национального стандарта ГОСТ «Кибербезопасность. Основные термины и определения», который раскроет и закрепит понятийный аппарат в этой важной области.

В результате этого термины, определения и понятийный аппарат должны обрести конкретную содержательную сущность, обеспечивающую однозначное взаимопонимание всех участников исследований, разработок и применения.

При этом необходимо учитывать особенность и перспективы современного этапа, заключающего в стремительном инновационном развитии и применении информационных технологий, таких как: 5G, 6G, SDN/NFV, «облачные вычисления» и виртуализация, «интернет вещи», eSIM технологии в мобильной связи и др., а также современных систем и средств защиты информации и информационного противоборства.

И очень важно для России на настоящем этапе разработать и принять, по аналогии с ведущими в этой области странами мира, основываясь на «Доктрине информационной безопасности Российской Федерации», такие национальные документы, как: Концепция, Стратегия и Политика кибербезопасности.

Учитывая исключительную важность этих документов следует полагать, что их разработка должна проходить под эгидой Совета Безопасности РФ по инициативе ПТН «Технологии кибербезопасности» и в соответствии с решением ВПК РФ или ее органов.

Эффективное решение этих задач и создает базовую основу обеспечения национальной безопасности Российской Федерации в международном пространстве.

### Заключение

В настоящей статье предпринята попытка с учетом особенностей современного этапа информационного противоборства раскрытия функциональной содержательной сущности термина и понятия «кибербезопасность». Предлагается схема соотношения (парадигмы) понятий «информационная безопасность» и «кибербезопасность» с учетом пересечения и дополнения их функциональных и предметных областей. На основании этого предлагаются уточненные варианты раскрытия (определения) термина «кибербезопасность», что должно, по нашему мнению, способствовать взаимопониманию участников в исследованиях и разработках и уточнению стоящих задач нормативно — методического и правового регулирования в этой области. Безусловно, статья носит дискуссионный характер и преследует цель обратить серьезное внимание на необходимость эффективной реализации и развития кибербезопасности Российской Федерации для обеспечения национальной безопасности в условиях современного и развивающегося информационного противоборства в международном сообществе.

**Литература**

1. Атагимова Э.И., Макаренко Г. И., Федичев А.В. Информационная безопасность. Терминологический словарь в определениях действующего законодательства. М., 2016, 448 с., ISBN 978-5-901167-28-1
2. Гаттаров Р.У. Концепция стратегии кибербезопасности // Вопросы кибербезопасности. 2014. № 1 (29). С. 2-4.
3. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1 (29). С. 2-9. DOI:10.21681/2311-3456-201-01-2-9
4. Алексеев Г., Смирнов И. Противоборство в киберпространстве по взглядам военно-политического руководства ведущих зарубежных государств, Зарубежное военное обозрение, №6, 2017 г., С.8-14.
5. Смирнов И., Якупов В. Противоборство в киберпространстве: направления развития сил и средств. Зарубежное военное обозрение, №3, 2018 г., С.13-18.
6. Башкиров Н. Взгляды военного и политического руководства США на защиту инфраструктуры от киберугроз. Зарубежное военное обозрение, №12, 2018 г., С.13-17.
7. Паршин С. Взгляды научного комитета МО США на классификацию угроз в киберпространстве. Зарубежное военное пространство, №5, 2017 г., С.12-17.
8. Бородакий Ю.В., Бутусов И.В., Добродеев А.Ю. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1). Вопросы кибербезопасности, №1 (1), 2013 г., С.2-9.
9. Бородакий Ю.В., Бутусов И.В., Добродеев А.Ю. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2). Вопросы кибербезопасности, №1 (2), 2014 г., С.5-12.
10. Добродеев А.Ю., Емельянов Г.В. О приоритетном технологическом направлении «Технологии кибербезопасности». Сборник материалов IV Межведомственной научно-практической конференции «Системы межведомственного информационного взаимодействия при решении задач в области обороны Российской Федерации», Национальный центр управления обороной Российской Федерации, г. Москва, 30 ноября 2018 г., С.90-97.
11. Ромашкина Н.П., Стефанович Д.В. Стратегические риски и проблемы кибербезопасности // Вопросы кибербезопасности. 2020. № 5(39). DOI:10.21681/2311–3456-2020-05-77-86
12. Журавель В.П. Противодействие угрозе кибертерроризма // Зарубежное военное обозрение. 2018. №5. с. 12-16.

# CYBERSECURITY IN RUSSIAN FEDERATION. A TRENDY TERM OR THE PRIORITY TECHNOLOGIC AREA OF ENHANCING NATIONAL AND INTERNATIONAL SECURITY OF THE XXI CENTURY

***Dobrodeev A. Yu.*[3]**

***The purpose of the article:*** *the study of the roleand and meaningof cybersecurity at the present stage of world development as the main factor for ensuring national and international security of the 21st century.*

***Research method:*** *synthesis and scientific forecasting, peer review, comparative analysis of the cybersphere within the system approach.*

***Results:*** *the state and ways of developing cybersecurity of leading foreign countries on the example of the United States, the state and ways of developing cybersecurity and cybersecurity technology in the Russian Federation are presented with justification for discussion proposals on the disclosure of the term and the concept of "cybersecurity."*

***Keywords:*** *cloud computing, internet stuff, virtualization, cyberspace, infosphere, information security, functional stability, information warfare, monitoring, computer attack, crypto-system, information protection system, paradigm, eSIM technology.*

**References**

1. Atagimova E`.I., Makarenko G. I., Fedichev A.V. Informatcionnaia bezopasnost`. Terminologicheskii` slovar` v opredeleniiakh dei`stvuiushchego zakonodatel`stva. M., 2016, 448 s., ISBN 978-5-901167-28-1
2. Gattarov R.U. Kontceptciia strategii kiberbezopasnosti // Voprosy` kiberbezopasnosti. 2014. № 1 (29). S. 2-4.
3. Romashkina N.P. Global`ny`e voenno-politicheskie problemy` mezhdunarodnoi` informatcionnoi` bezopasnosti: tendentcii, ugrozy`, perspektivy` // Voprosy` kiberbezopasnosti. 2019. № 1 (29). S. 2-9. DOI:10.21681/2311-3456-201-01-2-9

3 Alexandr Dobrodeev, Ph.D. , Senior Science Researcher, the Advisor of the General director, FGUP ZNIIS, Moscow, Russia. E-mail: a.dobrodeev@zniis.ru

4. Alekseev G., Smirnov I. Protivoborstvo v kiberprostranstve po vzgliadam voenno-politicheskogo rukovodstva vedushchikh zarubezhny` kh gosudarstv, Zarubezhnoe voennoe obozrenie, №6, 2017 g., S.8-14.
5. Smirnov I., Iakupov V. Protivoborstvo v kiberprostranstve: napravleniia razvitiia sil i sredstv. Zarubezhnoe voennoe obozrenie, №3, 2018 g., S.13-18.
6. Bashkirov N. Vzgliady` voennogo i politicheskogo rukovodstva SSHA na zashchitu infrastruktury` ot kiberugroz. Zarubezhnoe voennoe obozrenie, №12, 2018 g., S.13-17.
7. Parshin S. Vzgliady` nauchnogo komiteta MO SSHA na classifikatciiu ugroz v kiberprostranstve. Zarubezhnoe voennoe prostranstvo, №5, 2017 g., S.12-17.
8. Borodakii` Iu.V., Butusov I.V., Dobrodeev A.Iu. Kiberbezopasnost` kak osnovnoi` faktor natcional`noi` i mezhdunarodnoi` bezopasnosti XXI veka (chast` 1). Voprosy` kiberbezopasnosti, №1 (1), 2013 g., S.2-9.
9. Borodakii` Iu.V., Butusov I.V., Dobrodeev A.Iu. Kiberbezopasnost` kak osnovnoi` faktor natcional`noi` i mezhdunarodnoi` bezopasnosti XXI veka (chast` 2). Voprosy` kiberbezopasnosti, №1 (2), 2014 g., S.5-12.
10. Dobrodeev A.Iu., Emel`ianov G.V. O prioritetnom tekhnologicheskom napravlenii «Tekhnologii kiberbezopasnosti». Sbornik materialov IV Mezhvedomstvennoi` nauchno-prakticheskoi` konferentcii «Sistemy` mezhvedomstvennogo informatcionnogo vzaimodei`stviia pri reshenii zadach v oblasti oborony` Rossii`skoi` Federatcii», Natcional`ny`i` centr upravleniia oboronoi` Rossii`skoi` Federatcii, g. Moskva, 30 noiabria 2018 g., S.90-97.
11. Romashkina N.P., Stefanovich D.V. Strategicheskie riski i problemy` kiberbezopasnosti // Voprosy` kiberbezopasnosti. 2020. № 5(39). DOI:10.21681/2311–3456-2020-05-77-86
12. Zhuravel` V.P. Protivodei`stvie ugroze kiberterrorizma // Zarubezhnoe voennoe obozrenie. 2018. №5. s. 12-16.