ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РОССИИ И США В ИНФОРМАЦИОННОМ И КИБЕР-ПРОСТРАНСТВЕ: ПРАВОВЫЕ, ПОЛИТИЧЕСКИЕ И ЭКОНОМИЧЕСКИЕ АСПЕКТЫ

Виктор Володин*
Лилия Рожкова**
Ольга Сальникова***

DOI 10.24833/2073-8420-2017-4-45-59-68

Введение. *Проблема обеспечения безопасности страны, в том числе безопасности в информационной сфере, является ключевой в современных условиях развития глобального информационного пространства, что определяется долгосрочными национальными интересами страны в защите интересов общества, личности, государства от внешних и внутренних информационных угроз. Значительную актуальность обеспечение безопасности стран в информационной сфере приобретает в связи с участившимися в последнее время кибератаками, кибершпионажем, хищением информации, разглашением сведений, составляющих государственную тайну, вмешательством в частную жизнь и др. Особенно важным является защита мирового сообщества и стран от использования информационного пространства террористическими группировками в преступных целях, использования информационных технологий в военных и мирных целях при воздействии на массовое сознание. Цель исследования состоит в изучении правовых, политических, экономических механизмов, специфики подходов разных стран к обеспечению безопасности стран в информационном пространстве.*

Материалы и методы. *Реализация исследовательских задач была достигнута на основе изучения официальных документов, в том числе Доктрина информационной безопасности РФ 2016 г., Стратегия кибербезопаности США 2015 г., Резолюция ГА ООН от 4.12.2000 N 55/63 «Борьба с преступным использованием информационных технологий», Конвенция Совета Европы по киберпреступности 2001 г. Методология исследования базируется на системном подходе; использовались правовой, статистический методы.*

Результаты. *В статье рассмотрены подходы к обеспечению безопасности в мировом информационном пространстве – кибербезопаность и информационная безопасность; проанализированы мировые тенденции в области киберзащиты, российский рынок информационной безопасности; проведен комплексный*

* **Володин Виктор Михайлович**, доктор экономических наук, профессор, декан факультета экономики и управления Пензенского государственного университета. e-mail: ieu@pnzgu.ru.
** **Рожкова Лилия Валерьевна**, доктор социологических наук, доцент, профессор кафедры «Экономическая теория и международные отношения» Пензенского государственного университета. e-mail: econm@pnzgu.ru.
*** **Сальникова Ольга Владимировна**, старший преподаватель кафедры «Экономическая теория и международные отношения» Пензенского государственного университета. e-mail: econm@pnzgu.ru.

анализ американского подхода к обеспечению кибербезопасности и системы обеспечения информационной безопасности России; рассмотрены угрозы информационной безопасности РФ и кибербезопасности США.

Обсуждения и заключение. *Сегодня угрозы, которые связаны с использованием ИКТ в военно-политических и военно-стратегических целях исходят из мирового информационного пространства, а в последние годы они стали мощным дестабилизирующим фактором, который определяет направленность международных отношений. Это требует разработки правовой основы и международной системы контроля за обеспечением мировой информационной безопасности.*

Неотъемлемыми тенденциями современного мира является дальнейшее развитие процессов глобализации, формирование, трансформация глобальной информационной инфраструктуры. Для совершенствования и распространения принципов экономики знаний создаются соответствующие институты. В мировом масштабе это Глобальный совет по экономике знаний (GKEC - Global Knowledge Economics Council), разрабатывающий терминологию и стандарты. В свою очередь, для повышения эффективности использования знаний значительно расширяется спрос на новые технологии, особенно инфокоммуникационные. [21. С.112] Сегодня невозможно представить себе повседневную жизнь без развития и внедрения информационно-коммуникационных технологий (ИКТ) в разные сферы жизнедеятельности индивидов, общества, государства. Это приводит к появлению угроз внутреннего и внешнего порядка, исходящих из информационного пространства. Подчеркнем, что уровень развития национальных ИКТ, национальной информационной инфраструктуры оказывает непосредственное влияние на политический, экономический, оборонный потенциал стран. Именно поэтому перед каждой из стран стоит важная задача защиты своих национальных интересов в информационной сфере. Кроме того, развитие механизмов использования информационных технологий в военных целях, рост угроз от использования ИКТ террористическими группировками настоятельно требуют поиска международных способов и средств обеспечения информационной безопасности на глобальном уровне, формирования культуры поведения в информационном пространстве.

Актуальность поиска направлений обеспечения информационной безопасности подтверждают данные статистики. Ежегодно увеличивается число вредоносных объектов, обнаруживаемых в глобальной сети; их число исчисляется миллиардами, они распространяются больше, чем 100 млн интернет адресов и ежегодно увеличиваются на 40 % [1. С. 22].

Анализ научной литературы свидетельствует, что сегодня в мире присутствует два основных подхода к обеспечению безопасности в мировом информационном пространстве – это информационная безопасность (РФ, Китай и др.) и кибербезопасность (США и ее союзники). Несмотря на то, что эти подходы не являются взаимоисключающими, на практике они отличны по механизмам реализации интересов стран в информационном пространстве. Информационная безопасность более широкое понятие, чем кибербезопасность, в том числе рассматриваются и технические основы защиты информации, и вопросы влияния информации на индивидов, государство, общество. Исследователь П. А. Карасев отмечает важную особенность кибербезопасности, которая «… фактически «выводит за скобки» проблему вредоносного контента и использования ИКТ для оказания влияния на общественное сознание» [7. С 42]. Потребность в поиске баланса между обеспечением прав и свобод индивидов, тесно связанного с обеспечением национальной информационной безопасности выявили и последние международные события, так называемый «эффект Эдварда Сноудена». Таким образом, в США употребляется понятие «кибербезопасность», которое в основном относится к формированию безопасности архитектуры Интернета, в Китае (и в России) применяется термин «информационная безопасность», который предполагает оказание влияния на ограничения распространения нежелательной информации [2. С. 28].

Рассматривая мировые тенденции в области информационной безопасности и киберзащиты, мы видим, что по данным аналитической компании «IDC» в 2017 году во всем мире расходы на обеспечение киберзащиты достигнут $ 81,7 млрд, что на 8,2 % больше, чем в 2016 году. К 2020-му объем рынка превысит $100 млрд. [4]. По результатам глобального исследования корпоративной безопасности компании «Fortinet» можно выделить три ключевых фактора, которые способствуют формированию информационной безопасности как приоритетного направления. Это рост числа международных кибератак (WannaCry); рост нарушений безопасности (85 % организаций столкнулись с нарушениями в числе доминирующих из которых вредоносное ПО и программы-вымогатели – 47 % респондентов); рост давления со стороны регулирующих структур (требования законодательства о защите данных, в том числе штрафы за несоблюдение); переход к облачным технологиям, цифровая трансформация (требуют решения вопросов обеспечения безопасности облака) [12].

В соответствии с Доктриной информационной безопасности РФ 2016 г. она рассматривается как состояние защищенности государства, общества, личности от внутренних и внешних информационных угроз. При этом обеспечиваются: реализация прав и свобод индивидов, повышение и поддержание достойного уровня и качества жизни граждан, территориальная целостность, суверенитет, оборона и безопасность, устойчивое социально-экономическое развитие страны [3].

Систему обеспечения информационной безопасности РФ исследователи С.Е. Коротченко, М.Е. Листопад условно подразделяют на три блока. Во-первых, это правовая база; во-вторых, информационно-технический блок (программное и аппаратное обеспечение); в-третьих, экономический блок (разработка и совершенствование программ, средств, методов обеспечения информационной безопасности) [8. С. 147-148]. Нам представляется, что эта структура должна быть дополнена и политическим блоком, таким как разработка стратегических ориентиров обеспечения этой сферы, взаимодействие с членами мирового сообщества по снижению негативного влияния ИКТ на мировое информационное пространство. Важной задачей реализации российской национальной инновационной системы является ее интеграция в мировую экономику, в регионы, в которых имеются стратегические интересы для нашей страны [22. С. 111]. С.Е. Коротченко, М.Е. Листопад справедливо выделяют следующие сферы российской экономике, наиболее подверженные воздействию информационных угроз: национальная система статистики; кредитно-финансовая система; системы автоматизации учета органов исполнительной власти; российские предприятия, учреждения, организации, в том числе реализующие финансовые, биржевые, таможенные сделки [8. С. 148].

Рисунок 1 – Доля закрытых расходов в российском бюджете, % [16]

По оценкам аналитического центра «TAdviser», по итогам 2014 года объем российского рынка информационной безопасности составил 59 млрд руб. и вырос на 8 %. Лидером отечественных компаний в области обеспечения информационной безопасности продолжает оставаться «Лаборатория Касперского». В пятерку компаний также входят «Acronis», «Софтлайн», «Информзащита», «Оптима» [5]. Данные РБК свидетельствуют, что засекреченная часть российского бюджета в 2018 году останется на отметке в 17,61 % от общих расходов государственной казны. Доля закрытых расходов по разделу «Национальная безопасность и правоохранительная деятельность» увеличится до 38,27 % - максимума с 2007 года, но это будет компенсировано сокращением секретных частей «гражданских» разделов – «Национальная экономика» и «Общегосударственные вопросы» (рисунок 1) [16, 14].

Секретные расходы по разделу «Национальная оборона» в 2018 году останутся на уровне чуть ниже 66 %, как и в 2017-м (это единственный раздел бюджета, в котором секретных расходов больше, чем несекретных). Закрытые ассигнования увеличились по подразделу «Другие вопросы» национальной обороны: если в 2017 году их доля ожидается на уровне 59% (по показателям сводной бюджетной росписи), то в 2018 году запланирован 71 %. В федеральном бюджете есть подразделы, засекреченные на 100 % или почти на 100 %. Это ядерно-оружейный комплекс (раздел «Национальная оборона»), где никогда не было открытых расходов; подразделы «Органы пограничной службы» (100 %) и «Органы безопасности» (99,8%), к последним относятся ФСБ, ФСО, Федеральная служба по техническому и экспортному контролю (ФСТЭК) (рисунок 2) [16].

Следует отметить предпринимаемые в последнее время многочисленные попытки множества независимых аналитических компаний оценки информационной безопасности как отдельной экономической

Рисунок 2 – Доля закрытых расходов на национальную безопасность в бюджете, % [16].

категории. При этом основной проблемой выступает определение ключевых показателей и комплексный анализ взвешенной оценки информационной безопасности. Из года в год отмечается рост финансирования в рамках обеспечения информационной безопасности, что обусловлено ростом ущерба от потери данных. С. Е. Коротченко, М. Е. Листопад используют следующие данные для анализа факторов развития информационной безопасности в РФ: степень дифференциации субъектов РФ по показателям информационно развития (3,6 в 2011 г., 2,3 – в 2014 г.); доля организаций, которые применяют средства защиты информации в глобальных сетях (шифрование: 20111г. – 39,8% организаций, 2014 г – 39,3%), электронная подпись – 2011 г. – 73,9%, 2014 г. – 76,5%); доля населения, которое не использует интернет в силу соображений безопасности из общей численности россиян (2011 г. – 0 %; 2014 г. – 2,2%) [6, 8. С. 148].

Подход США к обеспечению кибербезопасности отличен от российского подхода. Он основан на понятии «киберпространство» - это сложная среда, которая не существует в физической форме и возникает в ходе взаимодействия индивидов, программного обеспечения (ПО), интернет сервисов с использованием устройств и сетей [1, с. 24]. М.М. Бескаравайный, А.Л. Татузов отмечают, что при анализе взаимосвязи киберпространства и инфраструктуры ИКТ, основное внимание уделяется не технологиям, а деятельности пользователей [1. С. 24]. Важным является то, что главное содержание киберпространства состоит в деятельности людей, использующих информационные ресурсы и ИКТ инфраструктуру. Киберпространство можно структурно анализировать через триаду его составляющих: информация в ее цифровом представлении; техническая инфраструктура, ИКТ, ПО; информационное взаимодействие субъектов путем использования информации, получаемой из сетей посредством технической инфраструктуры. В стандарте ИСО 27032:2012 кибербезопаность - это обеспечение конфиденциальности, целостности, доступности информации в современном киберпространстве.

Безопасность США в информационной сфере рассматривается в Стратегии кибербезопаности США 2015 года с широкой точки зрения как способность обеспечивать безопасность, защищать от кибератак свое киберпространство. В доктринальных документах США киберпространство рассматривается как полноценная сфера ведения военных действий, требующая принятия серьёзных мер для обеспечения защиты американских интересов и противодействия угрозам национальной безопасности США [18]. Киберпространство определяется как глобальная сфера, которая включает в себя взаимозависимые сетевые инфраструктуры: Интернет, телекоммуникационные и

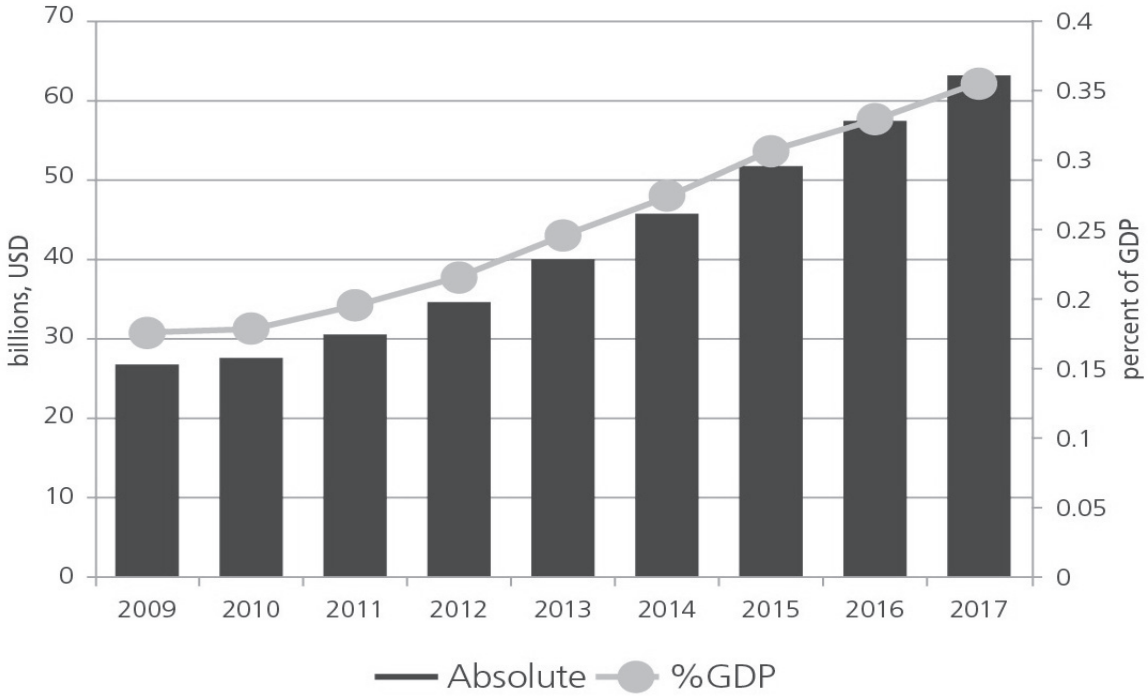

Рисунок 3 – Динамика бюджетных затрат США на информационные технологии и кибербезопасность в млрд долл, % от ВВП [9].

компьютерные сети. Следует подчеркнуть, что речь в этом случае идет, во-первых, о доступности, целостности, конфиденциальности информации, во-вторых, о стабильном функционировании среды и инфраструктуры. На рисунке 3 показана динамика бюджетных затрат США на кибербезопасность.

Прямые расходы на решение вопросов кибербезопасности (такие как брандмауэры и разведка угроз) неуклонно растут, приближаясь к 0,1% мирового ВВП и 0,35% ВВП США (см. рисунок 3). Эти силы могут стимулировать увеличение: способности атакующих выполнять все более сложные действия и рост активов, доступных через сети и, следовательно, уязвимых для атак.

Еще пятьдесят лет назад под эгидой Пентагона агентством исследовательских проектов *Advanced Research Projects Agency (ARPA)* стали разрабатываться программные технологий, которые должны были способствовать повышению технологического лидерства США. Созданная в США сеть *ARPANET* первоначально предназначалась для обмена информацией в случае возникновения глобального ядерного конфликта между США и СССР. Однако уже в то время спецслужбы США выделили реальное предназначение сети. Первая попытка передачи данных состоялась в 1969 г.; это событие положило начало развитию всемирной паутины. В 1990-м году *ARPANET* прекратила своё существование в связи с ее поглощением сетью *NSFNet*. Значительным событием было изобретение первого веб-браузера *worldwideweb*, который стал определять архитектуру современной мировой паутины.

Выход Интернета из тени Министерства обороны США, «подключение» к нему миллионов пользователей, размывание первоначально сугубо военного предназначения США, породило возникновение иллюзии, связанной с оценкой Интернета как уникального явления мировой истории, где реализуются базовые принципы свободы распространения информации и соблюдения прав и свобод личности. Миф о том, что интернет не может быть взят под контроль и управляться правительственными структурами и спецслужбами опровергает тот факт, что фактически вся мировая паутина выстроена на двух компонентах: организация *Internet Corporation for Assigned Names and Numbers (ICANN),* которая отвечает за присвоение сайтам интернет-адресов и шестнадцать корневых серверов, большая часть которых находится в США. Кроме того, *ICANN* – некоммерческая организация, поэтому многочисленные попытки «взять» её под международной контроль сталкиваются с сопротивлением США. Рассматривая систему информационной безопасности западных стран, можно заметить, что большая часть информационной инфраструктуры находится в руках частного сектора и управляется им. Это приводит к формированию некоторой модели взаимодействия, когда государство устанавливает свои правила, а граждане, придерживаясь этих правил, предпринимают попытки обезопасить себя. Следовательно, это идет на пользу США, так как это закрепляет позицию американского развития системы ИКТ и приводит к зависимости других государств от США.

Таким образом, сегодня наиболее острой проблемой в области обеспечения безопасности в информационной сфере является хранение большой информации о личных данных граждан государств, которые они предоставляют в глобальной сети Интернет. Персональные данные пользователей выступают своего рода параметрами, по которым можно оценивать состояние и динамику развития общественных систем, находить уязвимые места и оказывать на них давление. Отсюда вытекает, что информация носит глобальный характер. А персональные данные можно использовать в различных целях, в том числе и с целью накопления и последующего использования информации для проведения пропаганды.

Разные подходы к обеспечению безопасности РФ и США демонстрируют и их подходы к анализу информационных угроз и средств защиты от них [19, 20]. На рисунке 4 показаны основные угрозы информационной безопасности РФ и кибербезопаности США.

Следует отметить, что политика безопасности США в информационной сфере обусловлена совокупностью факторов. И прежде всего, это объективное превосходство страны как по уровню развития ИКТ, так и по степени «присутствия» в киберпространстве (по официальным документам США – это «новый театр военных действий»), что оказывает значительное влияние на формирование структуры мировой политики. Одним из свидетельств этого выступают вскрывшиеся и подтверждённые факты шпионажа и слежки, осуществляемые Агентством национальной безопасности США в Интернет сети. Для специалистов они не стали открытием, но способствовали акцентированию внимания на проблеме обеспечения безопасности человека, активизации политического дис-

курса на международном и национальном уровнях.

В различных международных соглашениях выделяется триада, источники международных информационных угроз: террористические группы, киберпреступники, государства. Следует подчеркнуть, что в рамках ООН неоднократно рассматривались вопросы борьбы с киберпреступностью. Резолюция ГА ООН (4.12.2000) раскрывает основные направления борьбы с киберпреступлениями: обязанность стран обеспечивать на уровне национального законодательства борьбу с этими правонарушениями; кооперация с правоохранительными органами при расследовании использования ИКТ в преступных целях; судебное преследование с координацией на мировой арене всеми государствами [13]. Принятие в 2001 г. Советом Европы Конвенции по киберпреступности стало воплощением этих направлений. Однако поскольку Конвенция была разработана ограниченным числом представителей из западных стран, она имеет особенность, связанную с реализуемым подходом обеспечения кибербезопаности. В ст. 32 (в) Конвенции присутствует положение, предусматривающее возможность проводить следственные мероприятия в сфере информационной инфраструктуры страны без наличия на это ее согласия. Это положение стало препятствием в ратификации Конвенции отдельными странами. Так, например, Россия не подписала эту конвенцию, не были согласованы приемлемые для РФ условия трансграничного доступа к компьютерным системам. Однако Россия предложила свой проект кибербезопасности,

Угрозы безопасности в информационной сфере: РФ и США

РФ

1. наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.
2. расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.
3. использование террористическими и экстремистскими организация механизмов информационного воздействия на индивидуальное, групповое и общественное сознание в целях создания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников.
4 рост компьютерной преступности, прежде всего в кредитно-финансовой сфере, рост числа преступлений, связанных с нарушением 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.

США

Ключевые киберугрозы

1 Теневые финансовые институты их активистские идеологические группы

2 Активизация негосударственных акторов (ИГИЛ, запрещенная в РФ)

Миссии доктрины кибербезопасности:

1 защита собственной информационной сети Пентагона и частных компаний; комплекс мер по сбору разведданных (агентства и зарубежные союзники), совместные операции с ФБР, ЦРУ с иностранными спецслужбами, в т. ч. создание системы автоматического обмена информацией; создание группы по кибербезопасности в Стратегическом командовании США (STRATCOM, объединяющий ядерные, космические войска и систему ПРО).

2 политика сдерживания интернет-угроз; киберподдержка военных операций США: через структуры *STRATCOM* интеграция «виртуальной реальности» с процессом создания военных планов, усиление роли интернета и компьютеризации в американской армии.

Стратегические цели «инструменты» миссий Пентагона:

1 систематизация кибербезопасности (привлечение квалифицированных кадров из рядов гражданских, создание прозрачных карьерных возможностей, разработка унифицированной технологической платформы операций и др.)

2 работа по конкретным дипломатическим направлениям - с союзниками на Ближнем Востоке, северо-западе Азии, в АТР и по линии НАТО.

Рисунок 4 – Угрозы информационной безопасности РФ и кибербезопаности США [3; 14; 9]

объясняющий то, что на современном этапе «регулирование» не охватывает в должном объёме отношения в области киберпространства как составляющей информационного пространства [15].

Следует подчеркнуть, что формирование и развитие мирового информационного пространства привело к наращиванию геополитического влияния путём использования ИКТ с целью информационного воздействия на массовое сознание, общественный и государственный порядок в разных странах, например, для смены в них политического режима [16, 17]. Сегодня США предпринимают значительные усилия для преобразования информационного пространства «под себя», в среду, создающую возможности свободной реализации преимуществ ИКТ для обеспечения своих национальных интересов. Другими словами США стремятся сохранить контроль над управлением Интернетом, рискуя лишиться свободного доступа в информационное пространство других стран, потерять политическое и экономическое влияние [10, 14]. Другие же страны выступают за интернационализацию управления Интернетом и контроль функций ICANN на международном уровне.

Сегодня угрозы, которые связаны с использованием ИКТ в военно-политических и военно-стратегических целях исходят из мирового информационного пространства. В последние годы они стали мощным дестабилизирующим фактором, который определяет направленность международных отношений. Необходимо отметить, что, признавая невозможность обеспечения кибербезопасности в одиночку, США проводят активную работу по сплочению союзников вокруг их понимания кибербезопасности, развития информационной инфраструктуры, использования ИКТ в военно-политических целях. При этом, понимая всю сложность системы глобального информационного пространства, США сотрудничают по некоторым вопросам обеспечения безопаности в информационной сфере с другими странами, принимают участие работе Группы правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной информационной безопасности. Это даёт надежду на согласование основных принципов международной информационной безопасности, разработку в перспективе единых международных норм поведения стран в киберпространстве.

Литература:

1. Бескаравайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопаности. 2014. № 1.
2. Булавин А.В. О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика, право. 2014. № 1.
3. Доктрина информационной безопасности Российской Федерации / Указ Президента РФ от 5.12.2016 № 646 // http://kremlin.ru.
4. Информационная безопасность (мировой рынок) 2017/07/05 // http://www.tadviser.ru.
5. Информационная безопасность (рынок России). 2016/12/15 // http://www.tadviser.ru.
6. Kamolov S.G. Digital public governance: trends and risks // Giornale di storia costituzionale. 2017. Т. 33. № 1.
7. Карасев П.А. Политика безопасности США в глобальном информационном пространстве: дисс. ...канд. полит. наук: 23.00.04. М., 2016.
8. Коротченко С.Е., Листопад М.Е. Развитие информационной безопасности России на современном этапе // Вестник НГИЭИ. 2016. № 9 (64).
9. Kempe F. Risk Nexus Overcome by cyber risks? Economic benefits and costs of alternate cyber futures // http://publications.atlanticcouncil.org.
10. Павлюк А.В. Административно-правовое регулирование экономики Российской Федерации в условиях экономических санкций // Пробелы в российском законодательстве. 2017. № 5.
11. Макаренко Г. Пентагон обновил стратегию кибербезопасности с учетом российской угрозы. 25.04.2015 // http://www.rbc.ru.
12. Панасенко А. 48% ИТ-руководителей не считают обеспечение ИБ приоритетным направлением // https://www.anti-malware.ru.
13. Резолюция ГА ООН от 4.12.2000 № 55/63 «Борьба с преступным использованием информационных технологий» // http://www.un.org.

14. Костенников М.В., Куракин А.В., Павлюк А.В. К вопросу о понятии и методах государственного управления в административном праве // NB: Административное право и практика администрирования. 2014. № 2.
15. Стратегии кибербезопасности Российской Федерации (проект концепции) от 10.01.2014 // Официальный сайт Совета Федерации РФ // http://www.council.gov.ru.
16. Ткачёв И., Фейнберг А. Секретные расходы бюджета по безопасности станут рекордными за 12 лет // http://www.rbc.ru.
17. Камолов С.Г. Проблемы развития экспорта России в переходный период. Диссертация на соискание ученой степени кандидата экономических наук. Москва, 1998.
18. U.S. National Security Strategy 2015. P. 7, 12–13. // National Security Strategy Archive // http://nssarchive.us.
19. Yengibaryan R. The institution of presidency in the USA // Giornale di Storia Costituzionale. Volume 33. Issue 1. 2017.
20. Yengibaryan R. Ethnicity and citizenship as key factors shaping human personality and behavior // Giornale di Storia Costituzionale. Volume 27. 2014.
21. Савостова Т.Л. Государственная кадровая политика и инновационное развитие России: концептуальные подходы: монография. М., 2016.
22. Савостова Т.Л., Бирюков А.Л. Институциональные механизмы стратегического партнерства России и Китая: инновационная интеграция // Экономика в промышленности. № 2. 2016.

ENSURING SECURITY OF THE RUSSIAN FEDERATION AND THE UNITED STATES IN THE INFORMATION AND CYBER SPACE: LEGAL, POLITICAL AND ECONOMIC ASPECTS

Introduction. *The issue of ensuring state security, including security in the information sphere, is critical in the current conditions for the development of global information space, which is determined by the country's long-term national interests in protecting interests of society, individuals and state from external and internal information threats. Ensuring state security in information sphere is becoming significantly relevant in connection with the increased number of cyber attacks, cyber espionage, theft of information, disclosure of information constituting state secrets, interference with privacy, etc. Protection of world community and countries from the use of information space by terrorist groups for criminal purposes, the use of information technologies for military or peaceful purposes by influencing mass consciousness are particularly important. The goal of the research is to explore law, political, economic mechanisms, and specifics of the countries' approaches to ensuring state security in the information space.*

Materials and methods. *The implementation of the research tasks was achieved through the study of official documents, including Doctrine of Information Security of the Russian Federation (2016), Cybersecurity Strategy of the USA (2015), UNGA Resolution No. 55/63 of 4 December 2000 "Combating the Criminal Use of Information Technologies", Convention Council of Europe on Cybercrime (2001). The research methodology is based on system approach; law and statistical methods.*

Results. *The article analyzes approaches to ensuring security in the global information space - cyber security and information security; contains analysis of world trends in the field of cyber defense, Russian market of information security; comprehensive analysis of the American approach to ensuring cyber security and ensuring system of information security in Russia; threats to Russia's information security and the USA's cyber security.*

Discussions and conclusion. *Today threats related to the use of ICT for military-political and military-strategic purposes come from global information space, and in recent years, they have become a powerful destabilizing factor that determines the focus of international relations. This requires the development of a legal framework and an international system for monitoring the global information security.*

Victor M. Volodin,
Doctor of Economic Sciences, Professor,
Dean of Faculty of Economics and Management, State University of the city of Penza
Lilia V. Rozhkova,
Doctor of Sociological Sciences, Professor, Department of Economic Theory and International Relations, State University of the city of Penza
Olga V. Salnikova,
Senior Lecturer, Department of Economic Theory and International Relations, State University of the city of Penza

Ключевые слова:
безопасность, информационное пространство, информационная безопасность, кибербезопаность, средства и механизмы обеспечения информационной безопасности, РФ, США

Keywords:
security, information space, information security, cyber security, means and mechanisms of information security ensuring, RF, USA

References:

1. Beskaravajnyj M.M., Tatuzov A.L., 2014. Kiberbezopasnost' – podhody k opredeleniyu ponyatiya [Cybersecurity - approaches to concept definition]. *Voprosy kiberbezopanosti [The Issues of Cybersecurity].* № 1.
2. Bulavin A.V., 2014. O podhodah SSHA i Kitaya k obespecheniyu kiberbezopasnosti [US and China approaches to cybersecurity support]. *Obshchestvo: politika, ehkonomika, pravo [Society: Politics, Economics, Law].* № 1.
3. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii [Doctrine of informational security] / Ukaz Prezidenta RF ot 5.12.2016 № 646. URL: http://kremlin.ru.
4. Informacionnaya bezopasnost' (mirovoj rynok) [Informational Security (world market)] 2017/07/05. URL: http://www.tadviser.ru.
5. Informacionnaya bezopasnost' (rynok Rossii) [Informational Security (Russian market)]. 2016/12/15. URL: http://www.tadviser.ru.
6. Kamolov S.G., 2017. Digital public governance: trends and risks. *Giornale di storia costituzionale [The Journal of Constitutional History].* Vol. 33. № 1.
7. Karasev P.A., 2016. Politika bezopasnosti SSHA v global'nom informacionnom prostranstve [American security policy in global informational space]: diss. ... kand. polit. nauk: 23.00.04. Moscow.
8. Korotchenko S.E., Listopad M.E., 2016. Razvitie informacionnoj bezopasnosti Rossii na sovremennom ehtape [The development of Russian informational security in the modern period]. *Vestnik NGIEHI.* № 9 (64).
9. Kempe F. Risk Nexus Overcome by cyber risks? Economic benefits and costs of alternate cyber futures. URL: http://publications.atlanticcouncil.org.
10. Pavlyuk A.V., 2017. Administrativno-pravovoe regulirovanie ehkonomiki Rossijskoj Federacii v usloviyah ehkonomicheskih sankcij [Administrative and legal regulation of the economy of the Russian Federation in the conditions of economic sanctions]. *Probely v rossijskom zakonodatel'stve [The Gaps in Russian Law].* № 5.
11. Makarenko G., 2015. Pentagon obnovil strategiyu kiberbezopasnosti s uchetom rossijskoj ugrozy [The Pentagon renews Cybersecurity strategy subject to Russian threat]. 25.04. URL: http://www.rbc.ru.
12. Panasenko A. 48% IT-rukovoditelej ne schitayut obespechenie IB prioritetnym napravleniem [48% IT- managers don't consider IS support as priority direction]. URL: https://www.anti-malware.ru.
13. Rezolyuciya GA OON ot 4.12.2000 № 55/63 «Bor'ba c prestupnym ispol'zovaniem informacionnyh tekhnologij» [Resolution adopted by the General Assembly [on the report of the Third Committee (A/55/593)] 55/63. "Combating the criminal misuse of information technologies"]. URL: http://www.un.org.
14. Kostennikov M.V., Kurakin A.V., Pavlyuk A.V., 2014. K voprosu o ponyatii i metodah gosudarstvennogo upravleniya v administrativnom prave [Approach to the subject of public administration concept and method in administrative law]. *NB: Administrativnoe pravo i praktika administrirovaniya [NB: Administrative law and administration practice].* № 2.
15. Strategii kiberbezopasnosti Rossijskoj Federacii (proekt koncepcii) ot 10.01.2014 [Strategies of cybersecurity of the Russian Federation]. URL: http://www.council.gov.ru.
16. Tkachyov I., Fejnberg A. Sekretnye raskhody byudzheta po bezopasnosti stanut rekordnymi za 12 let [Secret security expenses of budget will reach a record figure for the twelve years]. URL: http://www.rbc.ru.
17. Kamolov S.G., 1998. Problemy razvitiya ehksporta Rossii v perekhodnyj period [The topical issues of Russian export development in period of transition]. Dissertaciya na soiskanie uchenoj stepeni kandidata ehkonomicheskih nauk. Moscow.
18. U.S. National Security Strategy 2015. P. 7, 12–13. National Security Strategy Archive. URL: http://nssarchive.us.
19. Yengibaryan, R., 2017. The institution of presidency in the USA. *Giornale di Storia Costituzionale [The Journal of Constitutional History].* Volume 33. Issue 1.
20. Yengibaryan, R., 2014. Ethnicity and citizenship as key factors shaping human personality and behavior. *Giornale di Storia Costituzionale [The Journal of Constitutional History].* Volume 27.
21. Savostova T.L., 2016. Gosudarstvennaya kadrovaya politika i innovatsionnoe razvitie Rossii: kontseptual'nye podkhody: monografiya. [State personnel policy and innovative development of Russia: conceptual approaches/ monograph]. Moscow.
22. Savostova T.L., Biryukov A.L., 2016. Institutsional'nye mekhanizmy strategicheskogo partnerstva Rossii i Kitaya: innovatsionnaya integratsiya [Institutional Mechanisms for the Strategic Partnership Between Russia and China: The Innovative Integration]. *Ekonomika v promyshlennosti [Economy in the industry].* No. 2. April –June.