УДК 338.054.23

М. С. Кобышева
Управление «Экономической безопасности и противодействия коррупции»,
Санкт-Петербург, e-mail: marichinkoba@mail.ru

А. А. Володин
Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, e-mail: volodin.aa.spb@gmail.com

М. В. Иванов
Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, e-mail: ivanov_mv@spbstu.ru

Т. Ю. Феофилова
Санкт-Петербургский политехнический университет Петра Великого,
Санкт-Петербург, e-mail: feofilova_tyu@spbstu.ru

Т. М. Манасерян
Ереванский государственный университет, Ереван, e-mail: tatoulm@gmail.com

РИСКИ И УГРОЗЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Ключевые слова: кибербезопасность, киберпространство, цифровая экономика, экономическая безопасность, риски, угрозы, информационная безопасность.

Актуальность исследования обусловлена противоречием, заключающимся в фактическом существовании киберпространства, киберугроз, проблем обеспечения кибербезопасности и неспособности современной науки, включая теорию экономической безопасности, предоставить действенный инструмент для управления процессами, явлениями, действиями участников киберпространства. Цель исследования: на основе анализа проблем обеспечения экономической безопасности в киберпространстве, разработать предложения, направленные на учет и снижения опасности киберугроз. Объектом исследования является система экономической безопасности. Предметом исследования является кибербезопасность как элемент экономической безопасности. Основными методами исследования явились общенаучные анализ и синтез. Сформулировано авторское определение кибербезопасностью в контексте экономической безопасности, понимаемое как состояние киберпространства организации, при котором достигается баланс финансовых и иных ресурсов организации и заданного уровня сохранности информации, работы информационных систем и компьютерной техники, и обеспечивается экономическая безопасность посредством своевременного и эффективного противодействия киберугрозы. Выделены основные тенденции развития ИТ-технологий, рассматриваемых как источники угроз экономической безопасности. Определены проблемы институционального обеспечения кибербезопасности.

M. S. Kobysheva
Department of Economic Security and Anti-Corruption, St. Petersburg,
e-mail: marichinkoba@mail.ru

A. A. Volodin
Peter the Great St. Petersburg Polytechnic University, St. Petersburg,
e-mail: volodin.aa.spb@gmail.com

M. V. Ivanov
Peter the Great St. Petersburg Polytechnic University, St. Petersburg,
e-mail: ivanov_mv@spbstu.ru

T. Yu. Feofilova
Peter the Great St. Petersburg Polytechnic University, St. Petersburg,
e-mail: feofilova_tyu@spbstu.ru

T. M. Manaseryan
Yerevan State University, Yerevan, e-mail: tatoulm@gmail.com

RISKS AND THREATS TO THE ECONOMIC SECURITY OF RUSSIA IN THE CONDITIONS OF DIGITAL TRANSFORMATION

Keywords: cybersecurity, cyberspace, digital economy, economic security, risks, threats, information security.

The relevance of the study is due to the contradiction in the actual existence of cyberspace, cyber threats, cyber security problems and the inability of modern science, including the theory of economic security, to provide an effective tool for managing the processes, phenomena, actions of cyberspace participants. Purpose of the study. Based on the analysis of the problems of ensuring economic security in cyberspace, develop proposals aimed at taking into account and reducing the danger of cyber threats. The object of the research is the system of economic security. The subject of this research is cybersecurity as an element of economic security. The main research methods were general scientific analysis and synthesis. The author's definition of cybersecurity in the context of economic security is formulated, understood as the state of the organization's cyberspace, in which a balance of financial and other resources of the organization and a given level of information security, the operation of information systems and computer technology is achieved, and economic security is ensured through timely and effective countering the cyber threat. The main trends in the development of IT technologies, considered as sources of threats to economic security, are highlighted. The problems of institutional provision of cybersecurity are determined.

Введение

Решение проблем обеспечения экономической безопасность становятся рутинными для экономических субъектов вне зависимости от формы собственности и отраслевой принадлежности. В процесс обеспечения экономической безопасности вовлечен персонал, менеджмент и собственники в рамках функционала, закрепленного нормативными документами организаций. В последнее время наибольшее внимание уделяется рискам и угрозам, источниками которых является средства передачи информации и места ее хранения.

Пандемия 2020 затронула все страны, включая Российскую Федерацию. Новый вирус способствовал вовлечению широкого спектра экономических субъектов в цифровые экономические отношения. Следует отметить, что несмотря на наличие федеральной государственной программы «Цифровая экономика Российской Федерации», фактическая цифровизация экономики до момента пандемии практически не затронула субъектов малого и среднего бизнеса, которые, также, как и крупный бизнес, осознали остроту киберугрозы. Так, по данным Positive Technologies [1] превышение количества атак в начале 2020 года (1 кв.) превысило аналогичный показатель конца 2019 года (4 кв.) на 22,5%. И это речь идет только о тех атаках, которые были выявлены. Безусловно, рост количества атак был и в предшествующие периоды, однако не столь значительный.

Киберугрозы чаще всего рассматриваются как элемент системы информационной безопасности. Но в настоящее время этот поход требует корректировки, учитывая те последствия, которые субъекты экономики получают от реализации таких угроз. По данным Министерства внутренних дел РФ ущерб от киберпреступлений за девять месяцев 2019 г. превысил 10 млрд. рублей. Принимая во внимание темпы роста киберугроз при условии сохранения выявленной динамики, за 2020 г. ущерб составить более 16 млрд. рублей. Таким образом, считаем обоснованным рассматривать кибербезопасность как компонент системы экономической безопасности микро-, мезо- и макроэкономического уровня, а киберпространство как объект влияния рисков и угроз экономической безопасности.

Актуальность исследования обусловлена противоречием, заключающимся в фактическом существовании киберпространства, киберугроз, проблем обеспечения кибербезопасности и неспособности современной науки, включая теорию экономической безопасности, предоставить действенный инструмент для управления процессами, явлениями, действиями участников киберпространства.

Вопросы кибербезопасности неоднократно рассматривались в научных и научно-практических работах. В частности, обзор современных систем кибербезопасности представляют Dazhong Wu, Anqi Ren и другие [1], архитектуру систем кибербезопасности анализируют Lirim Ashiku and Cihan H Dagli [2]. Значительная часть работ посвящены моделированию безопасности в цифровой сфере экономики, к примеру работы Xiuwen Liu, Jianming Fu, Yanjiao Chen [3] и Angelo Corallo, Mariangela Lazoi, Marianna Lezzi [4]. В настоящее время российские исследователи и специалисты часто рассматривают вопросы создания прикладных кибернетических рисков, создаваемых современным развитием технологий. В частности, это работы Nashivochnikov, N.V.; Bolshakov, A.A. и других [5], а также Grishunin S., Suloeva S.

и других [6]. В существенная доля публикаций, рассматривают киберугрозы, кибербезопасность, как рискосодержащую часть экономической деятельности и экономической безопасности организации, к ним относятся работы Litvinenko A.N., Grachev A.V. и другие [7], Feorilova T.Yu., Litvinenko A.N. и другие [8].

Цель исследования: на основе анализа проблем обеспечения экономической безопасности в кибепространстве, разработать предложения, направленные на учет и снижения опасности киберугроз.

В соответствии с целью работы поставлены следующие **задачи**:

- уточнить понятие кибербезопасности в контексте экономической безопасности;
- выявить тенденции развития киберпространства с учетом рисков и угроз экономической безопасности;
- проанализировать институциональное обеспечение кибербезопасности;
- разработать предложения, направленные на совершенствование инструментов противодействия киберугрозам экономической безопасности.

Объектом исследования является система экономической безопасности.

Предметом исследования является кибербезопасность как элемент экономической безопасности.

Материал и методы исследования

В качестве информационных источников использованы работы российских и иностранных специалистов, рассматриваемых информационные аспекты экономической безопасности, киберпространство в структуре информационной безопасности, архитектуру киберпространства, киберугрозы и информационные риски экономической безопасности. Исследование базируется на статистических данных, полученных их заслуживающих доверия источников, касающихся криберугроз, киберпреступлений.

Среди основных методов исследования выбраны общенаучные анализ и синтез, которые позволили детализировать риски и угрозы экономической безопасности и выделить в них киберугрозы, а также систематизировать информацию, что позволило сформулировать предложения, направленные на повышение эффективности противодействия рискам и угрозам экономической безопасности, сформированных в киберпространстве.

Результаты исследования и их обсуждение

Анализ специализированной литературы показал, что в настоящее время не существует единообразного определения кибернетического, тоже относится и к определению виртуального пространства. Более того, в 2006 г. Хелен Джилл, являющаяся директором Национального научного фонда США по встроенным и гибридным системам, ввела в научно-практический оборот понятие «киберфизические системы», которое определила, как комплекс, состоящий из природных объектов, искусственных подсистем и контроллеров [9]. Таким образом, рассматривая информационное поле, включая средства передачи информации и ее хранение используются как минимум три понятия.

На институциональном уровне киберпространство, по нашим данным, определено однажды Верховным Судом США и трактуется, как «уникальная среда, не расположенная в географическом пространстве, но доступная каждому в любой точке мира посредством доступа в Интернет».

С точки зрения информационного права кибернетическое пространство характеризуется как: разнородное (гетерогенное) пространство, где каждый может свободно действовать, высказываться и работать (говоря образным языком – пространство «разума и свободы»); новое пространство человеческого самовыражения и общения; международное пространство, пересекающее любые границы; децентрализованное пространство, которым никакой оператор, никакое государство полностью не владеет и не управляет; глобальное объединения компьютерных сетей и информационных ресурсов, не имеющих четко определённого собственника и служащих для интерактивного соединения (коммуникации) физических и юридических лиц.

В проекте Стратегии кибербезопасности Российской Федерации определено киберпространство как сфера деятельности в информационном пространстве, образованную совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства), а кибербезопасность в свою очередь, как совокупность условий, при которых все составля-

ющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.

Кибернетическое пространство является относительно новой сферой деятельности, которую можно рассматривать со стороны пользователей и технологической стороны. С точки зрения пользователя, это пространство объединяет граждан многих стран, культур и профессий, собирающих, предлагающих и использующих разнообразную информацию, создавая некое интернациональное объединение. С технологической – эта система ничто иное как сложное техническое средство. Другими словами – это децентрализованная компьютерная сеть, которая с помощью имеющихся телекоммуникаций соединяет пользователей друг с другом посредством обмена информацией.

Неотъемлемы элементом кибепространства выступают киберугрозы. По результатам исследований научных работ установлено, что: 60% устройств обладают уязвимым веб интерфейсом; 70% наиболее часто используемых «умных» приборов, имеющих выход в сеть, уязвимы; 80% устройств подвержены утечке информации в той или иной степени и когда-то «выдавали» личную информацию о своих владельцах; 90% устройств собирают ту или иную персональную информацию о владельце без его ведома [9]. Происходят атаки не только на «компьютерные» системы, а на «реальные» (кардиостимуляторы, бытовые устройства, автотранспорт и т.д.).

Согласно отчета о глобальных рисках 2019 г. по мнению респондентам четвертое и пятое место по уровню опасности занимают кибератаки, в частности в форме кражи данных / денег (4 место) и в форме нарушения работы и инфраструктуры (5 место) [10]. Так поданным ИнфоБезопасность [11] только за сентябрь 2020 г. в РФ выявлено пять крупных утечек конфиденциальных данных. Согласно исследованию, которое провела «Лаборатория Касперского» в 2020 году расходы на кибербезопасность у крупного бизнеса сократились до 14 млн. долларов или на 26%, что на 4,9 млн долларов меньше уровня 2019 г. [12]. Респонденты связывают это снижение с расходами и убытками, возникшими в результате распространения коронавирусной инфекции и введённых ограничений. В малом бизнесе обратная тенденция, здесь расходы в 2020 году хоть незначительно, но выросли – на 8 тыс. долл. и составили 275 тыс. долл., что на 3% выше уровня 2019 г. Это факт косвенно свидетельствует о вовлечении субъектов малого бизнеса в цифровые экономические отношения и осознание опасности киберугроз для обеспечения приемлемого уровня экономической безопасности.

В исследованиях киберугрозы чаще всего трактуются как целенаправленное вредоносное воздействие на телекоммуникационные системы, системы сбора и обработки информации в критических областях, реализованные с помощью компьютерных и информационных технологий.

Характерными для киберугроз являются следующие признаки:

- целенаправленность атаки, даже в том случае, если оно осуществляется транзитивно через промежуточные узлы;
- использование широкого арсенал способов для достижения цели;
- применение суперкомпьютеров для создания новых сценариев атак, систем сканирования, вмешательства в управление производством, криптоанализа;
- привлечение независимых разработчиков для реализации атаки;
- борьба за контроль над глобальной инфраструктурой киберпространства.

Кибератаки отличаются от злонамеренных действий «обычных» нарушителей. Если традиционные злоумышленники в сети Интернет располагают весьма ограниченным арсеналом средств воздействия (вирусов, троянов, уязвимостей и эксплойтов), которые они пытаются, по возможности, применить к как можно более широкому классу систем, и ставят наиболее приоритетной целью охват «широкой аудитории», то киберугрозы, напротив, направлены на чётко ограниченный набор целей. Субъекты киберугроз располагают значительными ресурсами, которые они направляют на поиск путей, способов и механизмов воздействия именно на целевые системы. Отличие киберугроз определяется в основном тем, что при их реализации могут быть задействованы сервисы крупных компаний, владеющих системообразующими Интернет-ресурсами [9].

Таким образом, под кибербезопасностью в контексте экономической безопасности мы будем понимать состояние кибепространства организации, при котором достигается баланс финансовых и иных ресурсов организации и заданного уровня сохранности информации, работы информационных

систем и компьютерной техники, и обеспечивается экономическая безопасность посредством своевременного и эффективного противодействия киберугрозы.

И, прежде чем говорить о возможных путях решения проблем, стоит развеять стереотип, что данные проблемы можно отнести к задачам информационной безопасности. Хотя они и тесно взаимосвязаны, следует разграничить понятия информационной безопасности и кибербезопасности.

Для внедрения новых инструментов и методов обеспечения экономической безопасности организации требуется понимание тенденций развития информационных технологий.

Рассмотрим прогноз развития рынка информационных технологий в России (таблица).

В условиях постоянно растущего числа атак, создания механизмов их автоматизации, а также значительной зависимости информационной инфраструктуры и автоматизированных систем управления (в т.ч. военного и специального назначения) от электронных средств доступа и обмена информацией, ущерб даже от самых незначительных атак может быть катастрофическим.

Попытка проанализировать основные тенденции появления новых угроз безопасности и механизмов их осуществления, на современном этапе развития информационных технологий позволяет выявить следующие тенденции:

- появление новых типов компьютерных атак, характеризующихся смещением объекта воздействия от данных и программ к системам управления, направленным на вывод из строя информационных систем промышленного оборудования;

- целью современных атак является полный перехват управления и навязывание новых алгоритмов функционирования атакуемой системы;

- атака трансформируется в планируемую кибероперацию, направленную против тщательно выбранного объекта, и включающую предварительные этапы по подготовке, разработке средств преодоления защиты и обеспечению скрытности источника нападения;

- постоянно совершенствуются механизмы автоматизации доставки вредящего программного обеспечения от поиска уязвимостей и создании эксплойтов до методов социальной инженерии в социальных сетях. Появление специфической услуги hacking of service в виде сети сайтов и программных средств типа «Black hole» свидетельствует о том, что производство средств нарушения безопасности и их доставки превратилось в вполне легальную IT-отрасль [9].

Распространённые стратегические ИТ-тенденций в 2016 г. и 2019-2020 гг.

Тенденции 2016 г.	**Тенденции, которые реализуются в 2019-2020 гг.**
Развитие сетей устройств, состоящих из смартфонов, носимых гаджетов, потребительских и бытовых электронных устройств, транспортных средств и всевозможных датчиков	Авторами 20% всей корпоративной переписки станут роботы
Развитие сети устройств приведёт к необходимости соблюдения единого опыта пользовательского взаимодействия, который должен включать не только методы взаимодействия с электронными устройством, но и с виртуальной реальностью	Интернет вещей будет насчитывать около 6 млрд подключённых устройств
Развитие технологий 3D-печати со среднегодовым темпом роста 64,1% до 2019 г.	Автономные программные агенты будут участвовать в 5% всех экономических транзакций
Появление новых типов данных, например, сенсорной информации	Более чем 3 млн рабочими во всем мире будут управлять роботы-боссы
Глубокие нейронные компьютерные сети выйдут за пределы классических вычислительных систем и будут использоваться для создания систем, способных познавать и воспринимать окружающий мир самостоятельно и автономно	Каждое пятое «умное» здание (20%) испытывает на себе «цифровой вандализм», т.е. кибератаку
Машинное обучение приведёт к росту популярности роботов, автономных транспортных средств, виртуальных персональных ассистентов и умных советчиков, которые будут работать автономно или полуавтономно	В 50% быстрорастущих компаниях «умных» сотрудников будет меньше, чем «умных» машин

Сравнительный анализ [13,14].

Необходимость совершенствования механизма обеспечения кибербезопасности предполагает решение, как минимум, следующих задач:

- быть «на шаг впереди» по владению компетенциями в сфере кибербезопасности и технологий, обеспечивающими её, то есть анализировать и прогнозировать условия появления киберугроз и осуществлять мониторинг их реализации, формируя, тем самым базис для формирования новых компетенций;

- анализировать институциональную основу обеспечения кибербезопасности, методов её обеспечения в практике зарубежных стран и на этой основе разрабатывать, совершенствовать свои системы противодействия негативному влиянию киберугроз.

Однако несмотря на все очевидность поставленных задач, их выполнение осложнено рабом проблем, к которым следует отнести:

- отсутствие единого подхода к оцениванию уровня кибербезопасности;

- отсутствие общепризнанной проверенной методологии выявления, оценки, анализа, прогнозирования киберугроз;

- существенные различия в понимании ключевых категорий в области кибербезопасности, ее места в структуре системы экономической безопасности. А также системное регулирование отношений в киберпространстве на федеральном уровне управления.

Эффективное регулирование кибепространства должно обязывать его участников быть:

- этичными, т.е. деятельность лиц в кибернетическом пространстве должна осуществляться с соблюдением общепризнанных правовых принципов и базироваться на этических ценностях, среди которых: свобода слова; равный доступ к массовой информации и знаниям; обеспечение безопасности информационных продуктов и услуг; обеспечение защиты частной жизни и персональных данных; обеспечение защиты интеллектуальной собственности, культурного, языкового, межконфессионального разнообразия и др.;

- гибкими, логичными, технологичными: в процессе выработки национального права необходимо учитывать достижения технологического прогресса, экономическое и политическое положения каждой отдельной страны и всех участников кибернетического пространства;

- многообразными, т.е. не могут ограничиваться лишь одним решением, принятым раз и навсегда; помимо этого, в процессе выработки законодательства следует учитывать культурные и технические аспекты развития самой инфраструктуры глобальной коммуникации;

- универсальными: законодательные решения должны быть широко признаны; о них должны иметь представление все ключевые игроки рынка информационных товаров и услуг, в том числе это касается и технологически отсталых стран [15].

Анализируя современное российское законодательство, среди основных документов, определяющих институциональную основу обеспечения кибербезопасности в Российской Федерации, можно выделить, в первую очередь, следующие.

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [16]. Однако, в данном законе не определены понятия кибербезопасности, киберугроз и атак и т.п.

2. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года, которая содержит положение, предполагающее повышение эффективности международного сотрудничества в области противодействия преступности в сфере использования информационных и коммуникационных технологий» [17].

3. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». В доктрине сделан акцент на киберугрозы, в частности отмечена опасность возрастания масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличение числа 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 [18].

В развитие и для детализации перечисленных документов приняты ведомственные нормативные акты, которые формируют определенную систему требований по обеспечению информационной безопасности для информационных систем различного уровня.

Большие надежды у профессионального на Стратегию кибербезопасности Российской Федерации. Однако с 2013 г. этот документ находится в статусе проекта.

Вместе с тем, необходимо учитывать, что регулирование киберпространства исключительно на национальном уровне невозможно в силу его трансграничности. В связи с этим существует необходимость обозначения в российских документах, посвященных информационной безопасности, термина «кибербезопасность», что позволит установить соответствие между российскими и иностранными нормативными актами, а также даст возможность участвовать в международной нормотворческой работе в сфере кибербезопасности [19].

Заключение

В современном мире все меньше места остаётся узко специализированным проблемам. Большое значение приобретает исследование междисциплинарных предметных областей. К таким областям обоснованно относят обеспечение экономической безопасности, в которой значительное внимание в последнее время уделяется проблемам противодействия негативному влиянию киберугроз, способных нанести ущерб экономической системе различного уровня управления. Нами предпринята попытка обосновать кибербезопасность как элемент системы экономической безопасности и определить ее также через призму экономической безопасности. Основной акцент сделан на балансе ресурсов и обеспечения заданного уровня безопасности. Однако ресурсное обеспечение не ограничивается финансовыми или иными – материальными ресурсами. Необходима институциональная база регулирования экономических отношений в цифровом пространстве. При этом, установлено, что в настоящее время такая база не может рассматриваться как сформированная. Предстоит еще целенаправленная и скоординированная работа представителей различных отраслей науки для выработки единообразных основ функционирования участников киберпространства.

Библиографический список

1. Dazhong Wu, Anqi Ren, Wenhui Zhang, Feifei Fan, Peng Liu, Xinwen Fu, Janis Terpenny. Cybersecurity for digital manufacturing // Journal of Manufacturing Systems. 2018. Volume 48. Part C. P. 3-12.

2. Lirim Ashiku, Cihan H Dagli, System of Systems (SoS) Architecture for Digital Manufacturing Cybersecurity // Procedia Manufacturing. 2019. Volume 39. P. 132-140. DOI: 10.1016/j.promfg.2020.01.248.

3. Xiuwen Liu, Jianming Fu, Yanjiao Chen, Event Evolution Model for Cybersecurity Event Mining in Tweet Streams // Information Sciences. 2020. DOI: 10.1016/j.ins.2020.03.048.

4. Angelo Corallo, Mariangela Lazoi, Marianna Lezzi, Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts // Computers in Industry. 2020. Volume 114. P. 103165. DOI: 10.1016/j.compind.2019.103165.

5. Nashivochnikov N.V., Bolshakov A.A., Lukashin A.A., Popov M. The System for Operational Monitoring and Analytics of Industry Cyber-Physical Systems Security in Fuel and Energy Domains Based on Anomaly Detection and Prediction Methods // Studies in Systems. Decision and Control. 2020. P. 261-273. [Электронный ресурс]. URL: https://www.scopus.com/record/display.url?eid=2-s2.0-85075038014&origin=resultslist (дата обращения: 21.08.2020).

6. Grishunin S., Suloeva S., Nekrasova T., Egorova A. Development of the Mechanism of Assessing Cyber Risks in the Internet of Things Projects // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2019. P. 481-494. [Электронный ресурс]. URL: https://www.scopus.com/record/display.url?eid=2-s2.0-85072967126&origin=resultslist (дата обращения: 27.08.2020).

7. Litvinenko A.N., Grachev A.V., Guzikova L.A., Titov V.A. Shadow economy as object and subject of economic security // Proceedings of the 33rd International Business Information Management Association Conference. 2019. P. 7386-7393. [Электронный ресурс]. URL: https://www.scopus.com/record/display.url?eid=2-s2.0-85074104931&origin=resultslist (дата обращения: 11.07.2020).

8. Feorilova T.Yu., Litvinenko A.N., Grachev A.V. The socioeconomic system of a region as a source of threat to the national security of the Russian Federation // Proceedings of the 32nd International Business Information Management Association Conference. 2018. P. 6852-6860. [Электронный ресурс]. URL:https://www.scopus.com/record/display.url?eid=2-s2.0-85063040824&origin=resultslist (дата обращения: 11.08.2020).

9. От информационной безопасности к кибербезопасности. Опыт научно-исследовательских работ и подготовки кадров в Санкт-Петербургском политехническом университете Петра Великого / П.Д. Зегжда и др.; Санкт-Петербургский политехнический университет Петра Великого. СПб.: Изд-во Политехн. ун-та, 2017.

10. The Global Risks Report 2019. [Электронный ресурс]. URL: http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf (дата обращения: 01.08.2020).

11. Утечки и нарушение конфиденциальности данных в России. [Электронный ресурс]. URL: https://infobezopasnost.ru/blog/data-breach-russia/ (дата обращения: 11.08.2020).

12. Экономический аспект кибербезопасности. [Электронный ресурс]. URL: https://www.kaspersky.ru/blog/it-security-economics-2020-main/29179/ (дата обращения: 21.08.2020).

13. Актуальные киберугрозы: I квартал 2020 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q1/#id2 (дата обращения: 12.07.2020).

14. Ущерб от киберпреступлений превысил 10 миллиардов рублей [Электронный ресурс]. URL: https://rg.ru/2019/12/10/mvd-ushcherb-ot-kiberprestuplenij-prevysil-10-milliardov-rublej.html (дата обращения: 01.08.2020).

15. Рассолов И.М. Информационное право: учебник для магистров. 2-е изд., испр. и доп. М.: Юрайт, 2012.

16. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19.07.2018).

17. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года: приказ Президента: утв. Президентом РФ от 24.07.2013 № Пр-1753.

18. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646 // Собрание законодательства РФ. 2016. № 50. Ст. 7074.

19. Официальный сайт Совета Федерации. Проект «Концепция стратегии кибербезопасности Российской Федерации». [Электронный ресурс]. URL: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf. (дата обращения: 03.07.2020).