УДК 342.72/.73

Информационная безопасность в системе национальной безопасности Российской Федерации

Лось Лидия Викторовна

Старший преподаватель кафедры государственно-правовых дисциплин,
Российский государственный университет правосудия (Крымский филиал),
295000, Российская Федерация, Симферополь, ул. Павленко, 5;
e-mail: los_lidiya@mail.ru

Аннотация

В статье проводится анализ федерального законодательства по вопросам национальной безопасности, включая основные аспекты информационной безопасности. Автор обобщает подходы к пониманию безопасности, выделяя личную, общественную, национальную, глобальную. Особое внимание уделено правовым основам обеспечения информационной безопасности и перспективам усовершенствования законодательства, проблематике регулирования отношений в данной сфере.

Решение вышеперечисленных проблем состоит в усовершенствовании производимых и разрабатываемых отечественных информационных технологий, внедрении отечественных разработок, повышении эффективности научных исследований, повышения качества образования в сфере информационных технологий, повышении осведомленности граждан в вопросах обеспечения информационной безопасности. Важным направлением усовершенствования правовой сферы обеспечения информационной безопасности является организация деятельности по обобщению правоприменительной практики в этой сфере.

Таким образом, устойчивое развитие Российской Федерации и ее национальная безопасность, по сути, поставлены в прямую зависимость от надежности и безопасности функционирования информационно-телекоммуникационных сетей и информационных систем. Необходимо продолжить работу по усовершенствованию нормативно-правового регулирования обеспечения безопасности с учетом анализа правоприменительной практики.

Для цитирования в научных исследованиях

Лось Л.В. Информационная безопасность в системе национальной безопасности Российской Федерации// Вопросы российского и международного права. 2019. Том 9. № 3А. С. 159-170.

Ключевые слова

Безопасность, национальная безопасность, информационная безопасность, система обеспечения информационной безопасности, безопасность критической информационной инфраструктуры, государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, войска информационных операций.

Введение

С развитием информационных технологий и информационного общества, в условиях глобализации возник целый круг нерешенных вопросов и проблем, существенно изменилась характеристика вызовов и угроз цивилизации. Главные ценности, для защиты которых государства стремятся сформировать эффективные механизмы противодействия вызовам и угрозам, – мир, безопасность, права человека и устойчивое развитие [Умнова, Григорян, 2011].

Умнова И.А. к новым вызовам цивилизационного развития относит возрастание угроз миру и безопасности; расширение масштабов ущерба, приносимого окружающей среде; глобализацию экономического кризиса; рост социального неравенства и другие. К угрозам национальным интересам государств и обществ она относит: расширение международного терроризма и экстремизма, транснациональной преступности, обострение конфликтов между различными типами национальных культур, рост нищеты, болезней, поляризация общества в зонах вооруженных конфликтов и др. В этих условиях активизируется роль институциональных и правовых инструментов воздействия на общемировые и внутригосударственные процессы в целях формирования и защиты стабильного, справедливого и демократического миропорядка, строящегося на равноправных и партнерских отношениях между государствами [Умнова, Григорян, 2011].

Основная часть

Безопасность с момента возникновения человечества является важнейшей потребностью как индивида так и общества в целом. С философской точки зрения она выступает формой выражения жизнеспособности и жизнестойкости объектов материального мира. Однако столь упрощенное, чисто лингвистическое толкование данного понятия как отсутствие опасности или как «отсутствие угроз приобретенным ценностям**»,** или как условие жизнедеятельности личности, общества и государства представляется неправомерным, поскольку при этом как бы подразумевается возможность достижения подобной идеальной ситуации. Но в реальной жизни всегда существуют опасности самого различного характера. Поэтому категория «безопасность» - не абсолютна, а относительна и смысловое значение приобретает только в связи с конкретными объектами или сферой человеческой деятельности и окружающего мира [Абрамов, 2013].

В социальной практике все шире используется понятие «безопасность жизнедеятельности». Применительно к практическим потребностям под «безопасностью жизнедеятельности» понимается состояние защищенности материального мира и человеческого общества от негативных воздействий различного характера [Моисеева, 2016]. Как следует из этого определения, объектами безопасности жизнедеятельности являются человек, природа и общество.

В основу всякой классификации должны быть положены какие-то наиболее существенные признаки. Среди них, прежде всего, следует выделить объекты безопасности, характер угроз, сферы жизнедеятельности. В зависимости от объекта, жизненно важные интересы которого защищаются от внутренних и внешних угроз, выделяются, например, такие виды безопасности, как безопасность человека (личности), общества, государства, этнической группы (например, русскоязычного населения), государственных служащих и т.д.

Под безопасностью понимается такой уровень опасности, с которым на данном этапе научного и экономического развития можно смириться. Безопасность - это приемлемый риск. На практике полная безопасность недостижима, пока существует источник опасности. В соответствии с российской концепцией безопасность это состояние защищенности личности, общества и государства от внутренних и внешних угроз[1].

В зависимости от объекта угрозы можно выделить отдельные виды безопасности, такие как личная, общественная, национальная, глобальная.

Личная безопасность подразумевает защищенность людей, обусловленная индивидуальными качествами личности и используемыми ими средствами индивидуальной защиты. Под юридическим выражением личной безопасности понимается правовая возможность личности как субъекта права сохранить свое состояние безопасной жизнедеятельности, реализовать и сохранить которое обязуется государство. Колоткина О.А. объясняет природу личной безопасности тем, что «она суть, одна из основных витальных потребностей человека, без удовлетворения которой индивид не может нормально существовать, действовать и развиваться в социуме» [Колоткина, 2009]. Рассматривать безопасность личности следует в качестве комплексного института законодательства, включающего в себя как специализированные нормативно-правовые акты в сфере обеспечения безопасности личности, так и акты отраслевого характера.

Общественная безопасность обусловлена уровнем организации государственных структур и сознания людей. Наиболее сильным и жизнеспособным государство может стать только при наличии общенациональной идеи, поддерживаемой всем народом, основанной на единстве и межнациональном согласии. Поэтому проведение единой национальной политики является залогом обеспечения общественной безопасности [Амандыкова, Рустембекова, 2012]. Понятие общественной безопасности ранее содержалось в Приказе МВД РФ от 15 марта 2002 г. N 240 "Об утверждении Концепции развития Службы общественной безопасности МВД России»[2].Она определялась как состояние защищенности жизненно важных интересов личности, общества и государства от общественно опасных деяний и негативного воздействия чрезвычайных обстоятельств, вызванных криминогенной ситуацией в Российской Федерации, а также чрезвычайных ситуаций, вызванных стихийными бедствиями, катастрофами, авариями, пожарами, эпидемиями и иными чрезвычайными событиями.

В соответствии с Указом Президента РФ от 31 декабря 2015 г. N 683 «О Стратегии национальной безопасности Российской Федерации» национальная безопасность Российской Федерации это состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную,

[1] Указ Президента РФ от 31 декабря 2015 г. N 683 "О Стратегии национальной безопасности Российской Федерации" // Собрании законодательства Российской Федерации от 4 января 2016 г. N 1 (часть II) ст. 212

[2] Приказ МВД РФ от 15 марта 2002 г. N 240 "Об утверждении Концепции развития Службы общественной безопасности МВД России". Текст приказа официально публикован не был // http://base.garant.ru/1352745/

общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности.

Безопасность глобальная- защищенность планеты от внутренних (экологических, природных, техногенных) и внешних (космических, инопланетных) угроз, обеспечивается международным сотрудничеством и межгосударственными соглашениями.

Новые вызовы и угрозы, в том числе межцивилизационные коллизии, международный терроризм, мировой финансово-экономический кризис, энергетическая и информационная безопасность, природогенные, техногенные и социогенные катастрофы, климатические катаклизмы, пандемии и т.д. остро поставили вопрос о необходимости обеспечения качественно новой парадигмы глобальной безопасности. При этом проблематику международной безопасности, включая военно-политическую составляющую, ряд экспертов относит к традиционным форматам внешнеполитической деятельности.

Позицию России по данной проблеме предельно ясно сформулировал Д.А.Медведев в своем выступлении на международной конференции «Современное государство и глобальная безопасность» (Ярославль, 14 сентября 2009 г.): «Ответственность государств перед гражданами и друг перед другом, их эффективность в обеспечении общественной и глобальной безопасности - вот что нам необходимо». В итогах 2010 года (24 декабря 2010 г.) Президент России подчеркнул: «Безопасность нами понимается не только как внутренняя ситуация, хотя это, безусловно, очень важно, но и как глобальная безопасность» [Глобальная безопасность…, 2011].

Основные принципы и содержание деятельности по обеспечению безопасности приведены в Федеральном законе от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[3]. Данный Федеральный закон определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации.

Основными принципами обеспечения безопасности являются: соблюдение и защита прав и свобод человека и гражданина; законность; системность и комплексность применения публичными органами власти политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности; приоритет предупредительных мер в целях обеспечения безопасности; взаимодействие органов государственной власти с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Деятельность государства по обеспечению безопасности включает в себя:

1) прогнозирование, выявление, анализ и оценку угроз безопасности;

2) определение основных направлений государственной политики и стратегическое планирование в области обеспечения безопасности;

3) правовое регулирование в области обеспечения безопасности;

4) разработку и применение комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз безопасности, локализации и нейтрализации последствий их проявления;

[3] Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015) "О безопасности"//"Собрание законодательства РФ", 03.01.2011, N 1, ст. 2

5) применение специальных экономических мер в целях обеспечения безопасности;

6) разработку, производство и внедрение современных видов вооружения, военной и специальной техники, а также техники двойного и гражданского назначения в целях обеспечения безопасности;

7) организацию научной деятельности в области обеспечения безопасности;

8) координацию деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области обеспечения безопасности;

9) финансирование расходов на обеспечение безопасности, контроль за целевым расходованием выделенных средств;

10) международное сотрудничество в целях обеспечения безопасности;

11) осуществление других мероприятий в области обеспечения безопасности в соответствии с законодательством Российской Федерации.

Обеспечения информационной безопасности Российской Федерации является на сегодняшний момент одним из приоритетных элементов внешнеполитической стратегии российского государства. Поскольку эффективность информационной безопасности в значительной степени определяет место и роль любого государства в мировой политике, то правительство России начало уделять особое внимание реализации этой задачи в первой половине 2000-х годов [Назмутдинов, Попов, 2016].

Впервые Доктрина информационной безопасности Российской Федерации была принята в сентябре 2000 года, она стала системно-правовой основой для реализации тех целей и задач внешней политики России, которые связаны с защитой внутреннего информационного пространства государства и распространением позитивной информации о нем за рубежом. Подписанный Президентом России документ не являлся всеобъемлющим, но позволил сформулировать конкретные направления деятельности как публичных органов власти, так и средств массовой и сетевой информации. По истечении шестнадцати лет объективно возникла потребность сформулировать новуюсистему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Такой основой формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности стала Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646[4].В этом документе определены национальные интересы России в информационной сфере, проанализированы основные информационные угрозы и состояние информационной безопасности, намечены стратегические цели и основные направления обеспечения информационной безопасности, сформулированы организационные основы обеспечения информационной безопасности.

В данном нормативном акте впервые появилось понятие системы обеспечения информационной безопасности, которая стала частью системы обеспечения национальной безопасности Российской Федерации.Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

[4] Доктрина информационной безопасности Российской Федерации. Утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646 //Собрание законодательства Российской Федерации от 12 декабря 2016 г. N 50 ст. 7074.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Доктрина информационной безопасности Российской Федерации[5] определила стратегические цели и основные направления обеспечения информационной безопасности.

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Важнейшими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание

[5] Доктрина информационной безопасности Российской Федерации. Утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646 //Собрание законодательства Российской Федерации от 12 декабря 2016 г. N 50 ст. 7074.

политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры; в области стратегической стабильности и равноправного стратегического партнерства необходимо сформировать устойчивую систему неконфликтных межгосударственных отношений в информационном пространстве. В настоящее время эффективное правовое регулирование в данной сфере затруднено из-за отсутствия системообразующих законодательных актов, устанавливающих порядок отношений в сфере обеспечения безопасности критической информационной инфраструктуры в Российской Федерации.

В экономической сфере целями обеспечения информационной безопасности являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.

В области науки, технологий и образования целью обеспечения информационной безопасности является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности.

В рамках обеспечения государственной и общественной безопасности принят Федеральный закон от 26.07.17 № 187-ФЗ"О безопасности критической информационной инфраструктуры Российской Федерации"[6].

Данный закон определяет критическую информационную инфраструктуру Российской Федерации как совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия такихобъектов.

К объектам критической информационной инфраструктуры отнесены информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной промышленности, атомной промышленности, ракетно-космической промышленности, горнодобывающей промышленности, металлургической промышленности и химической промышленности. Правительством Российской Федерации в целях обеспечение безопасности критической информационной инфраструктуры Российской Федерации предложен комплекс мер правового, организационного, технического и иного характера, обеспечивающих устойчивое функционирование ее объектов в условиях проведения компьютерных атак.

Нанесение ущерба критической информационной инфраструктуре может привести к катастрофическим последствиям, а учитывая, что она является связующим звеном между другими секторами национальной инфраструктуры, неизбежно нанесет ущерб и этим секторам. Переход информационных и коммуникационных технологий на систему цифровых сигналов

[6] Федеральный закон от 26.07.17 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"// Собрание законодательства Российской Федерации № 31, 2017 г., ст.4736 (ч.1).

упростил и частично автоматизировал управление процессами, но в то же время, сделал их более уязвимыми перед компьютерными атаками. Вредоносная программа, направленная на внесение изменений в бинарный код программы (алгоритм программы, записанный в двоичной системе исчисления) способна вывести из строя любое оборудование, работающее с использованием бинарного кода. При этом равную опасность могут представлять атаки, совершаемые в преступных, террористических и разведывательных целях со стороны отдельных лиц, сообществ, иностранных специальных служб и организаций. За последние годы, исходя из различных методик оценки ущерба от вредоносных программ, он составлял от трехсот миллиардов до одного триллиона долларов, то есть от 0,4% до 1,4% общемирового ежегодного ВВП, и эти показатели имеют тенденцию к неуклонному росту. При развитии событий по наихудшему сценарию компьютерная атака способна полностью парализовать критическую информационную инфраструктуру государства и вызвать социальную, финансовую и экологическую катастрофу. Наращивание зарубежными странами информационно-технического воздействия является одной из проблем расширения информационного потенциала Российской Федерации. По данным Совета Безопасности за 2016 год было совершено более 70 миллионов кибератак, это в 3 раза больше, чем в 2015 году. При этом 60 % от всех кибератак совершены из-за рубежа[7].

Характерными примерами последствий негативного воздействия компьютерных атак на критическую инфраструктуру государства могут послужить остановка центрифуг иранской атомной станции с помощью компьютерного вируса StuxNet в сентябре 2010 г. и паралич работы нескольких крупных финансовых учреждений Южной Кореи в марте 2013 года.

В целях обеспечения информационной безопасности Российской Федерации и в соответствии с Указом Президента РФ от 15 января 2013г. N31c [5]и Концепцией государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации от 12.12.2014 г. № К 1274, утвержденной Президентом РФ[8] на Службу Безопасности Российской Федерации возложены полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации -информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

Государство должно предпринять все возможные меры, направленные на обеспечение своего информационного поля, необходимо создать «государственный штаб», который занимался бы не только защитой, экспертизой информационного потенциала, но и проведением планирования несанкционированных операций в информационном пространстве.

Вопрос о создании в Генеральном штабе Вооруженных сил войск информационных операций, для противодействия угрозам в информационной сфере возник еще в 2013 году. Но

[7] Пояснительная записка к проекту федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" Комитета Государственной Думы Федерального Собрания РФ по информационной политике, информационным технологиям и связи от 08.12.2016г.// http://asozd2.duma.gov.ru/main.nsf/%28Spravka%29?OpenAgent&RN=47571-7

[8] Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации от 12.12.2014 г. № К 1274 // http://base.garant.ru/71127868/

официального подтверждения до недавнего времени о создании этих войск не было. 14 января 2014 года Министр обороны Российской Федерации подписал приказ о создании в составе Генерального штаба Вооруженных сил России кибернетического подразделения, основной задачей которого является защита от несанкционированного вмешательства в информационные системы России. Этот приказ положил начало развития нормативно-правовой базы, касающейся обеспечения информационной безопасности стратегических национальных приоритетов.

22 февраля 2017 года министр обороны Российской Федерации на «Правительственном часе» в Госдуме подтвердил то, что в Вооруженных силах РФ созданы войска информационных операций – это формирование в российской армии, основными задачами которого является управление и защита военных компьютерных сетей, защита военных систем управления и связи от кибератак. Эти «информационные войска» призваны осуществлять координацию, проводимых информационными подразделениями, операций, проводить экспертизу информационного потенциала Минобороны РФ, расширять возможности в информационном пространстве, а также обеспечение надежной защиты проходящей в военных системах информации, защита компьютерных сетей военного назначения, проведение разведки, в том числе и создание разведывательного поля. На войска информационных операций также возложено решение проблем кибератак, выявление и предупреждение информационных атак, выявление и предотвращение атак в террористических целях. Эти войска призваны осуществлять обеспечение устойчивого развития инфосферы страны. Войска информационных операций являются структурным подразделением Вооруженных сил РФ. Они непосредственно подчиняются Министерству обороны РФ. В эти войска входят части и подразделения в военных округах и на флотах, в которых работают математики, программисты, инженеры, офицеры радиоэлектронной борьбы и другие.

К основным задачам, требующим немедленного решения, относится необходимость нормативно-правового регулирования противодействия использованию потенциала информационных технологий, угрожающих интересам государства. Создание информационных войск сопровождается рядом проблем в различных сферах деятельности. В экономическом плане это развитие отечественных технологий, например, в развитии электронной компонентной базы, программного обеспечения, вычислительной техники, средств связи, уступает зарубежному. Поэтому остается зависимость в экономическом плане от других стран. В научном аспекте, состояние информационной безопасности характеризуется недостаточным количеством научных исследований, направленных на создание перспективных информационных технологий. Проблемным является кадровое обеспечение в области информационной безопасности, так как эффективность проведения мероприятий в этой области зависит от уровня теоретической и практической подготовки сотрудников. Кроме этого, важной проблемой является малоэффективное использование региональных информационных ресурсов, недостаточный уровень и возможность свободного доступа граждан к открытым государственным информационным ресурсам.

Заключение

Эти проблемы характерны не только для войск информационных операций, но и для всей системы защиты информационного пространства. Трудности в экономической, научной, кадровой сфере предопределяют необходимость постоянного совершенствования нормативно-правового регулирования информационной безопасности.

Решение вышеперечисленных проблем состоит в усовершенствовании производимых и разрабатываемых отечественных информационных технологий, внедрении отечественных разработок, повышении эффективности научных исследований, повышения качества образования в сфере информационных технологий, повышении осведомленности граждан в вопросах обеспечения информационной безопасности. Важным направлением усовершенствования правовой сферы обеспечения информационной безопасности является организация деятельности по обобщению правоприменительной практики в этой сфере.

Таким образом, устойчивое развитие Российской Федерации и ее национальная безопасность, по сути, поставлены в прямую зависимость от надежности и безопасности функционирования информационно-телекоммуникационных сетей и информационных систем. Необходимо продолжить работу по усовершенствованию нормативно-правового регулирования обеспечения безопасности с учетом анализа правоприменительной практики.

Библиография

1. Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015) "О безопасности"//"Собрание законодательства РФ", 03.01.2011, N 1, ст. 2
2. Федеральный закон от 26.07.17 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"// Собрание законодательства Российской Федерации № 31, 2017 г., ст. 4736 (ч.1).
3. Указ Президента РФ от 31 декабря 2015 г. N 683 "О Стратегии национальной безопасности Российской Федерации" // Собрании законодательства Российской Федерации от 4 января 2016 г. N 1 (часть II) ст. 212
4. Доктрина информационной безопасности Российской Федерации. Утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646 //Собрание законодательства Российской Федерации от 12 декабря 2016 г. N 50 ст. 7074.
5. Указ Президента РФ от 15 января 2013 г. N 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"// Собрание законодательства Российской Федерации от 21 января 2013 г. N 3 ст. 178
6. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации от 12.12.2014 г. № К 1274 // http://base.garant.ru/71127868/
7. Приказ МВД РФ от 15 марта 2002 г. N 240 "Об утверждении Концепции развития Службы общественной безопасности МВД России". Текст приказа официально публикован не был // http://base.garant.ru/1352745/
8. Пояснительная записка к проекту федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" Комитета Государственной Думы Федерального Собрания РФ по информационной политике, информационным технологиям и связи от 08.12.2016г.// http://asozd2.duma.gov.ru/main.nsf/%28Spravka%29?OpenAgent&RN=47571-7
9. И.А.Умнова, С.А. Григорян Мир, безопасность и устойчивое развитие как высшие ценности в современном государстве и праве // Научно-практический журнал «Наука и образование: хозяйство и экономика; предпринимательство; право и управление», 2011, сентябрь.
10. И.А. Умнова Право мира.- М.: Эксмо, 2010.
11. В.В. Абрамов. Дефиниция «безопасность» в гражданском праве и законодательстве // Вестник Пермского университета, 2013, №4(22).
12. Колоткина О.А. Право личности на безопасность: понятие и механизмы обеспечения в РФ: теоретико-правовое исследование. Автореф. …канд.юрид.наук. Саратов, 2009.
13. Амандыкова С.К., Рустембекова Д.К. Обеспечение национальной безопасности как вектор государственной национальной политики Республики Казахстан (конституционно-правовые аспекты) / Конституционное право и политика: Сборник материалов международной научной конференции: Юридический факультет МГУ им. М.В. Ломоносова. 28 - 30 марта 2012 года / Отв. ред. С.А. Авакьян. М., 2012. С. 686.
14. Глобальная безопасность: инновационные методы анализа конфликтов. Под ред. Смирнова А.И. – М.: Общество «Знание» России. 2011. - 272 с.
15. Назмутдинов Т.Р., Попов К.Г. Современная концепция информационной безопасности в Российской Федерации: состояние и перспективы развития. VIII Международная студенческая электронная научная конференция «Студенческий научный форум» - 2016. Уфа, 2016.
16. Моисеева Е.К. Сборник лекций по дисциплине «Безопасность жизнедеятельности и медицина катастроф». 2016 // https://medic.studio/meditsina-katastrof-knigi.html.

The information safeguard in the system of national security of the Russian Federation

Lidiya V. Los'

Senior lecturer at the Department of the state and legal disciplines,
Russian State University of Justice (Crimean branch),
295000, 5, Pavlenko st., Simferopol, Russian Federation;
e-mail: los_lidiya@mail.ru

Abstract

The article analyzes the Federal legislation on the questions of national security, including the main aspects of information safeguard. The author generalizes approaches to the understanding of security, highlighting personal, public, national and global. The particular attention is paid to the legal basis of information safeguard and the prospects for improving legislation and also the issues of the regulation of relations in this area.

For citation

Los' L.V. (2019) Informatsionnaya bezopasnost' v sisteme natsional'noy bezopasnosti Rossiyskoy Federatsii [The information safeguard in the system of national security of the Russian Federation]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 9 (3A), pp. 159-170.

Keywords

Security, national security, information safeguard, information security system, security of critical information infrastructure, the state system of detection, the prevention and elimination of the computer attacks' consequences on the information resources of the Russian Federation, troops of information operations.

References

1. Federal'nyj zakon ot 28.12.2010 N 390-FZ (red. ot 05.10.2015) "O bezopasnosti"// "Sobranie zakonodatel'stva RF", 03.01.2011, N 1, st. 2
2. Federal'nyj zakon ot 26.07.17 N 187-FZ "O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii"// Sobranie zakonodatel'stva Rossijskoj Federacii № 31, 2017 g., st.4736 (ch.1).
3. Ukaz Prezidenta RF ot 31 dekabrya 2015 g. N 683 "O Strategii nacional'noj bezopasnosti Rossijskoj Federacii" // Sobranii zakonodatel'stva Rossijskoj Federacii ot 4 yanvarya 2016 g. N 1 (chast' II) st. 212
4. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii. Utverzhdennaya Ukazom Prezidenta RF ot 5 dekabrya 2016 g. № 646 //Sobranie zakonodatel'stva Rossijskoj Federacii ot 12 dekabrya 2016 g. N 50 st. 7074.
5. Ukaz Prezidenta RF ot 15 yanvarya 2013 g. N 31s "O sozdanii gosudarstvennoj sistemy obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak na informacionnye resursy Rossijskoj Federacii"// Sobranie zakonodatel'stva Rossijskoj Federacii ot 21 yanvarya 2013 g. N 3 st. 178
6. Koncepciya gosudarstvennoj sistemy obnaruzheniya, preduprezhdeniya i likvidacii posledstvij komp'yuternyh atak na informacionnye resursy Rossijskoj Federacii ot 12.12.2014 g. № K 1274 // http://base.garant.ru/71127868/
7. Prikaz MVD RF ot 15 marta 2002 g. N 240 "Ob utverzhdenii Koncepcii razvitiya Sluzhby obshchestvennoj bezopasnosti MVD Rossii". Tekst prikaza oficial'no publikovan ne byl // http://base.garant.ru/1352745/
8. Poyasnitel'naya zapiska k proektu federal'nogo zakona "O bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii" Komiteta Gosudarstvennoj Dumy Federal'nogo Sobraniya RF po informacionnoj politike, informacionnym tekhnologiyam i svyazi ot 08.12.2016g.// http://asozd2.duma.gov.ru/main.nsf/%28Spravka%29?OpenAgent&RN=47571-7

9. I.A. Umnova, S.A. Grigoryan Mir, bezopasnost' i ustojchivoe razvitie kak vysshie cennosti v sovremennom gosudarstve i prave [Peace, Security and Sustainable Development as Highest Values in the Modern State and Law] // Nauchno-prakticheskij zhurnal «Nauka i obrazovanie: hozyajstvo i ehkonomika; predprinimatel'stvo; pravo i upravlenie» [Scientific and Practical Journal “Science and Education: Economy and Economics; entrepreneurship; law and management”], 2011, sentyabr'.
10. I.A. Umnova Pravo mira [Peace law].- M.: EHksmo, 2010.
11. V.V. Abramov. Definiciya «bezopasnost'» v grazhdanskom prave i zakonodatel'stve [The definition of “security” in civil law and legislation] // Vestnik Permskogo universiteta [Bulletin of Perm Universit], 2013, №4(22).
12. Kolotkina O.A. Pravo lichnosti na bezopasnost': ponyatie i mekhanizmy obespecheniya v RF: teoretiko-pravovoe issledovanie. Avtoref. …kand.yurid.nauk. [The right of an individual to safety: the concept and mechanisms of security in the Russian Federation: a theoretical and legal study. Author's abstract ... Ph.D] Saratov, 2009.
13. Ensuring national security as a vector of state national policy of the Republic of Kazakhstan (constitutional and legal aspects) [Amandykova S.K., Rustembekova D.K. Obespechenie nacional'noj bezopasnosti kak vektor gosudarstvennoj nacional'noj politiki Respubliki Kazahstan (konstitucionno-pravovye aspekty)] / Konstitucionnoe pravo i politika: Sbornik materialov mezhdunarodnoj nauchnoj konferencii: YUridicheskij fakul'tet MGU im. M.V. Lomonosova. 28 - 30 marta 2012 goda [Constitutional law and policy: Collection of materials of the international scientific conference: Law Faculty of Moscow State University. Mv Lomonosov. March 28 - 30, 2012] / Otv. red. S.A. Avak'yan. M., 2012. S. 686.
14. Global'naya bezopasnost': innovacionnye metody analiza konfliktov. Pod red. Smirnova A.I. [Global security: innovative methods for analyzing conflicts. Ed. Smirnova A.I.] – M.: Obshchestvo «Znanie» Rossii [Society "Knowledge" of Russia]. 2011. - 272 s.
15. Nazmutdinov T.R., Popov K.G. Sovremennaya koncepciya informacionnoj bezopasnosti v Rossijskoj Federacii: sostoyanie i perspektivy razvitiya. VIII Mezhdunarodnaya studencheskaya ehlektronnaya nauchnaya konferenciya «Studencheskij nauchnyj forum» [The modern concept of information security in the Russian Federation: state and development prospects. VIII International Student Electronic Scientific Conference "Student Scientific Forum"] - 2016. Ufa, 2016.
16. Moiseeva E.K. Sbornik lekcij po discipline «Bezopasnost' zhiznedeyatel'nosti i medicina katastrof». [Collection of lectures on the subject "Life Safety and Disaster Medicine."] 2016 // https://medic.studio/meditsina-katastrof-knigi.html.