Международная информационная безопасность в рамках международного права (методология, теория)

Костенко Н. И.,
доктор юридических наук,
профессор, старший научный сотрудник Научно-исследовательского центра Краснодарского высшего военного училища имени генерала армии С. М. Штеменко Министерства обороны РФ, член Всемирной ассоциации международного права
E-mail: prof_48kost@mail.ru

Аннотация. *Целью исследования является формирование основных подходов к становлению и развитию права международной информационной безопасности.*

Актуальность подобного анализа обеспечивается анализом юридической природы права международной информационной безопасности. Исследуется информационная составляющая, которая служит важным компонентом международной и национальной безопасности. Исследуются вопросы регулирования международной информационной безопасности в рамках международного права в целом и международной информационной безопасности в частности. Анализируются проблемы обеспечения международной информационной безопасности по совершенствованию правовой системы международной информационной безопасности. Анализируется юридическая природа международной информационной безопасности в современных условиях. Исследуются подходы к предмету образования новой формирующейся отрасли международного права — право международной информационной безопасности.

В работе задействованы общенаучные и частно-научные методы исследовательской деятельности, включающие в себя анализ, синтез, дедуктивный, индуктивный, системный методы, нормативно-логический метод и иные методы познания.

В статье особым образом показана роль информационной безопасности на международном уровне. Субъектами обеспечения международной информационной безопасности являются государство, его органы, юридические и физические лица, которые осуществляют свою деятельность в указанной сфере.

Современная система информационной безопасности является всеобъемлющей, и она охватывает не только политические, правовые, военные, экономические, но и экологические, гуманитарные направления с выходом на международный уровень.

Новизной исследования является то, что, во-первых, международная информационная безопасность направлена на формирование и обеспечение международно-правового режима информационной безопасности на основе общепризнанных принципов и норм международного права и международных договоров. Во-вторых, международно-правовые принципы и нормы, регулирующие правовое положение информационного пространства, порядок его использования публичными лицами, относятся к отрасли международного права — праву международной информационной безопасности. В-третьих, под международной информационной безопасностью понимают защищённость глобальной информационной системы от «триады угроз» — террористических, киберпреступных и военно-политических (под военно-политическими угрозами подразумеваются информационные войны и информационное противоборство). В-четвертых, международная информационная безопасность регулируется общепризнанными принципами и нормами международного права, международными договорами Российской Федерации и может претендовать на признание в качестве новой отрасли международного права — права международной информационной безопасности.

Ключевые слова: *информационная безопасность, задачи, принципы, информационное пространство, субъекты, государства, международное сообщество.*

На сегодняшний день защита национальных интересов в информационной сфере на международном уровне зависит от конкретного государства, его структур, общества, индивида и не застрахована от внешних и внутренних угроз.

Международная информационная безопасность в полной мере зависит от информационного пространства. Информационное пространство — сфера деятельности, которая связана с хранением информации, использованием, созданием, формированием, преобразованием,

передачей информации и оказывает воздействие как на индивидуальное, так и общественное сознание[1].

Информационная составляющая служит важным компонентом национальной безопасности. В силу своей многогранности информационная безопасность затрагивает различные сферы общественной жизнедеятельности. Она является неотъемлемой частью военной безопасности и не замыкается в ее рамках. Информационная безопасность не ограничивается сугубо техническими и технологическими параметрами (информационно-техническая безопасность)[2].

На рубеже XX-XXI вв. в России было повышенное внимание как к национальной, так и к международной информационной безопасности. Причинами всему этому явились сложности вхождения России в глобальное информационное пространство, что объясняется прежде всего отставанием России в развитии информационного общества.

Сегодня на национальном уровне информационная безопасность расценивается как одно из важных направлений формирования национальной политики России. Государственная национальная политика обязана обеспечить безопасность в области распространения и получения информации.

Обеспечение информационной безопасности любого взятого государства на национальном уровне, на наш взгляд, неотделимо от обеспечения её на международном уровне.

Субъектами обеспечения международной информационной безопасности являются государство, его органы, юридические и физические лица, которые осуществляют свою деятельность в указанной сфере.

Вопросы регулирования международной информационной безопасности должны развиваться в рамках международного права.

Сегодня глобальный характер информационного взаимодействия способствует образованию целого ряда проблем информационной безопасности[3].

Средства обеспечения международной информационной безопасности образуются совокупностью правовых, материальных и др., которые необходимы для осуществления противодействия угрозам.

Значимость указанных направлений для Российской Федерации подчёркивается в целом ряде документов, таких как: Стратегия национальной безопасности Российской Федерации до 2020 г., Стратегия развития информационного общества Российской Федерации от 07.02.2008, Концепция внешней политики Российской Федерации от 30.11.2016, Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. и Доктрина информационной безопасности Российской Федерации от 05.12.2016. Целесообразно отметить, что доктрина информационной безопасности представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере, отражает изменившуюся ситуацию в мире в связи с развитием информационных технологий. Спектр угроз расширился и смещается в сферу коммуникационных сетей и бытовых цифровых технологий.

Сегодня Интернет является пространством международной информационной политики. В международной «паутине» возникают ростки военных угроз, военных конфликтов, о чем в Доктрине информационной безопасности РФ прямо говорится, что спецслужбы отдельных стран с государственным размахом используют информационные технологии в злонамеренных целях и это представляет очевидную угрозу суверенитету России и благополучию граждан. На сегодняшний день наряду со старыми методами угроз со стороны экстремистов и наркоторговцев, компьютерных взломщиков и мошенников появились новые сетевые угрозы, например, угрозы межгосударственного противостояния. Понятие «кибервойна» стало не игрушкой подростков и футурологов, а фактором международных отношений. Всё это ещё раз заставляет задуматься о создании международной структуры ООН по регулированию и функционированию сети Интернет.

Принятие Федерального закона от 29.06.2015 № 188-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”» в части введения государственного регулирования в сфере использования российских программ для электронных вычислительных машин или баз данных было своевременным и крайне необходимым.

Указом Президента РФ от 09.05.2017 утверждена Стратегия развития информационного общества в Российской Федерации на 2017-2030 гг. (далее —Стратегия 2017). Стратегия 2017 является формированием не только

[1] Капустин А.Я. Угрозы международной информационной безопасности: формирование концептуальных подходов // Журнал российского права. 2015. № 8. С. 89-100.

[2] Марков А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник СПбУ. Сер. 12. Вып. 1. С. 43-48.

[3] Исабаев Б. Международно-правовой уровень обеспечения информационной безопасности // Вестник КазНУ. 2011. С. 34-37.

позитивной модели информационного общества, связанной с развитием общества знания, но и модели негативной, формируемой в результате усилий геополитических конкурентов Российской Федерации. Положения Стратегии 2017 не только направлены на решение проблемы технологической безопасности, ускорение экономического развития и модернизацию социальной сферы, они ориентированы на масштабное совершенствование законодательства, что позволяет ее оценивать как манифест политико-правового развития страны в цифровую эпоху.

М. Радыш приходит к выводу, что национальная безопасность государств во многом стала зависеть от способности государств обеспечить надлежащий уровень информационной безопасности[4].

Думается, что на сегодняшний день для обеспечения международной информационной безопасности необходимо совершенствование международной и национальной правовой системы. И такая система обязана обеспечивать международную информационную безопасность.

Совершенствование самой системы международной информационной безопасности сможет защищать информационные ресурсы и информационно-телекоммуникационную инфраструктуру от воздействия информационного оружия, использования информационных технологий в современных киберпреступлениях.

12.10.2018 в очередной раз Российская Федерация официально внесла на рассмотрение Генеральной ассамблеи ООН проект резолюции по информационной безопасности. Данная резолюция нацелена на принятие мировым сообществом правил ответственного поведения государств в информационном пространстве, акцентирует внимание на исключительно мирном использовании информационно-коммуникационных технологий, неприменении силы, невмешательстве во внутренние дела других государств, уважении государственного суверенитета и предотвращении конфликтов в этой сфере.

Резолюция призвана оградить цифровую среду «от клеветников, провокаторов» и действий стран, «которые, пользуясь технологическим преимуществом, хотят диктовать волю другим государствам». У российского проекта есть уже 12 стран-соавторов, «совокупное население которых составляет четверть жителей планеты»[5].

А.В. Крутских и А.А. Стрельцов полагают, что растущее число стран выражает солидарность с Россией в том, что в настоящее время возникла потребность разработки под эгидой ООН конвенции по борьбе с преступностью в информационной сфере, которая исключала бы наиболее противоречивые положения Будапештской универсальной конвенции, учитывала ее положительный опыт и одновременно гарантировала суверенитет и невмешательство во внутренние дела государств. Необходим документ глобального охвата, учитывающий позиции всех стран и основанный на уважении принципа государственного суверенитета[6].

С другой стороны, информационная сфера способна обеспечить реализацию стратегических национальных приоритетов всего мирового сообщества.

В данной ситуации интересы государств и мирового сообщества в информационной сфере выражены в обеспечении выполнения принципов международного права и обеспечении безопасности государства и международного сообщества от информационной войны, информационного терроризма, киберпреступности и агрессии как в мирное, так и в военное время.

Реализация указанных направлений в целом и любого из них в отдельности представляет собой достаточно сложную задачу, которую необходимо решать государствам и мировому сообществу комплексно.

Полагаем, что укрепление международной информационной безопасности будет способствовать сохранению территориальной целостности государств, упрочению суверенитета, защите государственной тайны и развитию международного сотрудничества. Возникающие ежедневные информационные угрозы нуждаются в оперативном научном исследовании причин и условий совершения новых международных преступлений (информационные войны, информационный терроризм и разного вида киберпреступления).

На сегодняшний день мировое сообщество, доверившись многим объектам инфраструктуры вычислительных систем, оказалось беззащитно перед прямыми угрозами.

Цель прямых угроз — уничтожение жизненно важных объектов без применения военной боевой силы.

Одновременно с этим усиливается деятельность спецслужб государств, осуществляющих техническую разведку в отношении государственных органов, научных организаций и предприятий оборонно-промышленного комплекса и вооружённых сил государства.

[4] Радыш М. Белая книга российских спецслужб. М.: Обозреватель. 2016. С. 113.

[5] Россия внесла в ГА ООН проект резолюции по информационной безопасности // URL.: https://tass.ru/politika/5686030 (дата обращения: 20.11.2018).

[6] Крутских А.В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. 2014. № 11. С. 5-8.

Активизируется различными террористическими и экстремистскими организациями пропаганда экстремистской идеологии. В противоправных целях активно создаются средства деструктивного воздействия на объекты информационной инфраструктуры.

Возрастают масштабы компьютерной преступности, прежде всего, в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением международных стандартов прав и свобод человека и гражданина. Методы, способы и средства совершения таких киберпреступлений становятся все изощреннее.

А. В. Морозова и Т. А. Полякова считают, что деятельность государств в информационном пространстве должна гарантировать свободу технологического обмена и свободу обмена информацией с учётом уважения суверенитета государств, существующих политических, исторических и культурных особенностей[7].

В настоящее время сотрудничество между государствами по вопросам международной информационной безопасности осуществляется в форме международных договоров. Например, 08.05.2015 между Правительством Российской Федерации и Правительством Китайской Народной Республики подписано Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. В преамбуле данного Соглашения подтверждается, что государственный суверенитет и международные нормы и принципы, вытекающие из государственного суверенитета, распространяются на поведение государств в рамках их деятельности, связанной с использованием информационно-коммуникационных технологий, а также юрисдикцию государств над информационной инфраструктурой на их территории. В то же время государство имеет суверенное право определять и проводить государственную политику по вопросам, связанным с информационно-телекоммуникационной сетью Интернет, включая обеспечение безопасности.

Согласно Соглашению первой среди основных угроз международной информационной безопасности является использование информационно-коммуникационных технологий для осуществления актов агрессии, направленных на нарушение суверенитета, безопасности, территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

В число приоритетов российско-китайского сотрудничества также входит совместная борьба с использованием информационно-коммуникационных технологий в террористических и иных противоправных целях.

В практическом плане Соглашение предполагает обмен информацией о существующих и потенциальных рисках и угрозах в сфере международной информационной безопасности, взаимодействие по совершенствованию международно-правовой базы сотрудничества в данной области, разработку и осуществление необходимых совместных мер укрепления доверия и др.

Среди прочих важных направлений взаимодействия документ предполагает проведение совместных научных исследований по вопросам, связанным с обеспечением международной информационной безопасности, совместную подготовку специалистов в этой сфере, обмен студентами, аспирантами и преподавателями, а также контакты на экспертном уровне в различных форматах.

20.11.2013 подписано Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в области обеспечения информационной безопасности. Согласно ст. 3 стороны организуют взаимодействия и сотрудничество по следующим основным направлениям:

— разработка нормативных правовых актов для проведения совместных скоординированных мероприятий в информационном пространстве, направленных на обеспечение информационной безопасности в государствах — участниках Соглашения;

— трансформация нормативных актов и методических документов государств — участников Соглашения, регламентирующих отношения в сфере обеспечения информационной безопасности;

— организация трансграничной передачи информации;

— совершенствование технологии защиты информационных систем и ресурсов от потенциальных и реальных угроз;

— анализ и оценка угроз информационной безопасности информационных систем;

— совершенствование деятельности в области выявления и нейтрализации устройств и программ, представляющих опасность для функционирования информационных систем;

— реализация согласованных мероприятий, направленных на недопущение несанкционированного доступа к информации, размещённой в информационных системах, и ее утечки по техническим каналам.

В рамках работы Межпарламентской ассамблеи СНГ 28.11.2014 приняты модельные законы: модельный закон СНГ «Об информации, информатизации и обеспечении информационной безопасности» и модельный закон «О критически

[7] Морозова А. В., Полякова Т. А. Организационно-правовое обеспечение информационной безопасности. М.: РПА Минюста России, 2013. С. 251.

важных объектах информационно-коммуникационной инфраструктуры».

Модельный закон «Об информации, информатизации и обеспечении информационной безопасности» содержит понятие «критически важная информационно-коммуникационная инфраструктура» — совокупность средств и систем формирования, создания, преобразования, передачи, использования и хранения информации, отказ или разрушение которых могут оказать существенное отрицательное воздействие на национальную безопасность.

Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры» содержит понятия:

— «информационно-коммуникационная инфраструктура» — совокупность территориально распределённых государственных и корпоративных информационных систем, сетей связи, средств коммутации и управления информационными потоками, а также организационных структур и нормативно-правовых механизмов регулирования, обеспечивающих их эффективное функционирование;

— «критически важные инфраструктуры» — объекты, системы, службы и институты, разрушение или выведение из строя которых может нанести серьёзный ущерб социальному, экономическому или политическому порядку, или национальной безопасности;

— «критический элемент критически важного объекта информационно-коммуникационной инфраструктуры» — структурный компонент критически важного объекта информационно-коммуникационной инфраструктуры, выход из строя которого с неизбежностью приводит к нарушению или прекращению функционирования объекта в целом;

— «объект информационно-коммуникационной инфраструктуры» — совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения функционирования такого объекта, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, а также персонала, который осуществляет их эксплуатацию.

Решением Совета глав правительств СНГ 28.10.2016 утверждена Стратегия сотрудничества государств — участников СНГ в построении и развитии информационного общества на период до 2025 года и План действий по ее реализации. Из Стратегии усматривается, что использование информационно-коммуникационных технологий является одним из приоритетов и необходимым условием повышения качества жизни граждан, развития экономической, социально-политической и культурной сфер жизни общества, а также совершенствования системы государственного управления.

Хорошей основой для выстраивания обеспечения информационной безопасности служат межправительственные соглашения о сотрудничестве в этой сфере. В частности, Россия уже заключила соглашения с Бразилией, Белоруссией и Кубой.

Одно из первых международных соглашений в области обеспечения международной информационной безопасности было подписано 16.06.2009 в Екатеринбурге Правительствами государств — членов Шанхайской организации сотрудничества — Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. В Соглашении обращается внимание на их деятельность, которая должна способствовать социальному и экономическому развитию и быть совместимой с задачами поддержания международной безопасности и стабильности. Деятельность Шанхайской организации сотрудничества должна соответствовать общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека, а также принципам регионального сотрудничества и невмешательства в информационные ресурсы государств сторон.

11.07.2014 в ходе визита Президента РФ В. В. Путина в Республику Куба министры иностранных дел РФ и Республики Куба подписали в присутствии глав государств двустороннее межправительственное Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. Подписание Соглашения стало важным шагом на пути к формулированию общих подходов к проблемам международной информационной безопасности. Оно выводит на новый уровень отношения наших государств в данной сфере. Российско-кубинское сотрудничество в области обеспечения международной информационной безопасности будет осуществляться по таким важным направлениям, как выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, разработка и осуществление совместных мер доверия, формирование согласованной политики в области международной информационной безопасности, обеспечение информационной безопасности критически важных объектов, борьба с использованием информационно-коммуникационных технологий в террористических и иных преступных целях, содействие обеспечению безопасного, стабильного функционирования и интернационализации управления сетью Интернет.

Соглашение создаёт нормативно-правовую базу для осуществления практического взаимодействия ведомств государств. В рамках реализации Соглашения Россия и Куба будут проводить на регулярной основе межведомственные консультации для обмена информацией об угрозах информационной безопасности, а также координации совместных мер реагирования на такие угрозы.

Вместе с тем, на сегодняшний день в научной литературе отсутствует единообразное понимание предмета права международной информационной безопасности, а сам термин не является устоявшимся. Однако это никоим образом не уменьшает важность его теоретического осмысления, а практическое значение дискуссии по этому вопросу определяется, среди прочего, потребностями его исследования как научной дисциплины.

Е.С. Зиновьева, исследуя понятие «международная информационная безопасность», полагает, что это нельзя считать целью одного государства, так как под ней следует понимать основные приоритеты, ориентиры, к которым должно стремиться все мировое сообщество[8].

В то же время она считает, что под международной информационной безопасностью в терминологии ООН понимают защищённость глобальной информационной системы от так называемой «триады угроз» — террористических, преступных и военно-политических (под военно-политическими угрозами подразумеваются информационные войны и информационное противоборство)[9]. Этой же позиции придерживается Е.С. Полевина[10] .

А.А. Ефремов приходит к выводу и считает, что под международной информационной безопасностью понимается совокупность международных и национальных институтов, призванных регулировать деятельность различных субъектов глобального информационного пространства[11].

Обращает на себя внимание то, что концептуальные подходы, сформировавшие понятие «международная информационная безопасность», находят своё отражение в тексте Совместного заявления об общих вызовах безопасности в начале XXI в., которое было подписано президентами России и США 02.09.1998. Данное заявление способствовало конституированию вопросов международной информационной безопасности в качестве объекта теории международных отношений[12].

Понятие международной информационной безопасности характеризуется объектом международной информационной безопасности, угрозами безопасности этого объекта, субъектами обеспечения международной информационной безопасности, деятельностью данных субъектов и используемыми ими средствами[13].

Можно полагать, что объектом международной информационной безопасности являются государственные национальные интересы в информационной сфере, в которой играет большую роль международная информация.

По мнению А.А. Стрельцова и А.И. Смирнова, в современных условиях укрепление российско-американского сотрудничества по-прежнему является одним из ключевых факторов обеспечения международной безопасности вообще и в информационной сфере в частности[14].

Международная информационная безопасность сегодня определяется как «состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве»[15].

Из проведённого краткого анализа усматривается следующее:

во-первых, международная информационная безопасность направлена на формирование и обеспечение международно-правового режима информационной безопасности на основе общепризнанных принципов и норм международного права и международных договоров;

во-вторых, международно-правовые принципы и нормы, регулирующие правовое положение информационного пространства, порядок его использования публичными лицами, относятся к новой отрасли международного права — праву международной информационной безопасности;

---

[8] Зиновьева Е.С. Международная информационная безопасность. М.: МГИМО-Университет, 2013. С. 118-123.

[9] См.: там же.

[10] Пелевина Е.С. Особенности системы информационной безопасности как элемента международной безопасности в современном мире // Теории и проблемы политических исследований. 2017. Т. 6. № 1А. С. 194-205.

[11] Ефремов А.А. Защита государственного суверенитета РФ в информационном пространстве. М.: Норма, 2017. С. 109-111.

[12] См.: http://www.conventions.ru/view_base.php?id=14315/ (дата обращения: 21. 11. 2018).

[13] Крылов Г.О. Международный опыт правового регулирования информационного регулирования Российской Федерации: Автореф. дисс. … канд. юрид наук. М., 2007. С. 6-7.

[14] Смирнов А.И. Российско-американское сотрудничество в области международной информационной безопасности: предложения по приоритетным направлениям // Международная жизнь. 2017. № 11. С. 72-81.

[15] Док. Генеральной Ассамблеи ООН A/55/40. Средства и системы технического обеспечения обработки, хранения и передачи информации // https://moodle.kstu.ru/mod/page/view.php?id=28916 (дата обращения: 21 11.2018).

в-третьих, под международной информационной безопасностью понимают защищённость глобальной информационной системы от «триады угроз» — террористических, киберпреступных и военно-политических (под военно-политическими угрозами подразумеваются информационные войны и информационное противоборство).

Все изложенное выше будет положено в основу развития новой отрасли международного права — права международной информационной безопасности — и позволит охватить значительный пласт научных исследований по следующим направлениям:

— информационное оружие как новое оружие, применяемое в военно-политических целях, противоречащих международному праву;

— осуществление враждебных действий и актов агрессии, направленных на дискредитацию суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

— применение информационного оружия в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды идей терроризма и вовлечения новых субъектов в террористическую деятельность;

— применение информационного оружия для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей или теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию;

— применение информационного оружия для совершения преступлений, в том числе связанных с неправомерным доступом к компьютерной информации, с созданием, использованием и распространением вредоносных компьютерных программ;

— информационная война, информационный терроризм и киберпреступления разных составов и агрессии как в мирное, так и в военное время — новый вид международных преступлений третьего тысячелетия.

Таким образом, право международной информационной безопасности представляет систему принципов и норм, регулирующих отношения субъектов международного права в целях обеспечения международной информационной безопасности, безопасности информации и защиту информации государства и других субъектов международного права как в мирное, так и военное время, предотвращения информационной войны, информационного терроризма, киберпреступности и агрессии, а также защищённости информационно-телекоммуникационной инфраструктуры, включая компьютеры и находящуюся в них информацию.

Список литературы

1. Ефремов А. А. Защита государственного суверенитета РФ в информационном пространстве. М.: Норма, 2017. 128 с.
2. Исабаев Б. Международно-правовой уровень обеспечения информационной безопасности // Вестник КазНУ. 2011. 234 с.
3. Зиновьева Е. С. Международная информационная безопасность. М.: МГИМО-Университет, 2013. С. 118-123.
4. Капустин А. Я. Угрозы международной информационной безопасности: формирование концептуальных подходов // Журнал российского права. 2015. № 8. С. 89-100.
5. Крылов Г. О. Международный опыт правового регулирования информационного регулирования Российской Федерации: Автореф. дисс. … канд. юрид. наук. М., 2007. С. 6-7.
6. Крутских А. В., Стрельцов А. А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. 2014. № 11.
7. Марков А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник СПбГУ. Сер. 12. Вып. 1. С. 43-48.
8. Морозова А. В., Полякова Т. А. Организационно-правовое обеспечение информационной безопасности. М.: РПА Минюста России, 2013. 276 с.
9. Пелевина Е. С. Особенности системы информационной безопасности как элемента международной безопасности в современном мире // Теории и проблемы политических исследований. 2017. Т. 6. № 1А. С. 194-205.
10. Радыш М. Белая книга российских спецслужб. М.: Обозреватель. 2016. С. 113.
11. Смирнов А. И. Российско-американское сотрудничество в области международной информационной безопасности: предложения по приоритетным направлениям // Международная жизнь. 2017. № 11. С. 72-81.
12. Стратегический вектор обеспечения международной информационной безопасности. СПб.: СПИИ РАН, 2016. 122 с.

International Information Security in the Framework of International Law (Methodology, Theory)

Kostenko N. I.,
Doctor of Law, Professor,
Senior Researcher of the Research Center of the Krasnodar Higher Military School named after Army General S. M. Shtemenko of the Ministry of Defense of the Russian Federation,
Member of the World Association of International Law
E-mail: prof_48kost@mail.ru

Abstract. *The aim of the study is to form basic approaches to formation and development of the law of international information security. The relevance of such an analysis is provided by the analysis of the legal nature of international information security. Examines the information component, which is an important component of international and national security. Explores the international information security management issues within the framework of the law of international law and of international information security in particular. Examines the problem of ensuring international information security on the improvement of the legal system of international information security.*

Analyses the legal nature of international information security in modern conditions. Explores approaches to the subject of education newly emerging branch of international law: the right of international information security. The work involves scientific and private scientific research methods, including analysis, synthesis, deductive, inductive, systematic methods, normative-logical method and other methods of cognition. In an article in a special way the role of information security at the international level and of ensuring international information security actors are the State, its bodies, legal entities and natural persons, who are required to carry out its activities in a specified direction.

The novelty of the study is: firstly, the international information security is aimed at forming and ensuring international information security legal regime on the basis of the universally recognized principles and norms of international law and international treaties; secondly, international legal principles and norms regulating the legal status of the information space, usage of public persons, belong to the branch of international law: the right of international information security; thirdly, under the international information security understand global information system security from threats of «triad»- terrorist, kiberprestupnye and politico-military (under military-political threats means information warfare and information confrontation). Fourthly, the international information security is governed by universally recognized principles and norms of international law, international treaties of the Russian Federation and.

Keywords: *information security, tasks, principles, information space, entities, states, the international community.*

References

1. Efremov A. A. Zaschita gosudarstvennogo suvereniteta RF v informatsionnom prostranstve. M.: Norma, 2017. 128 s.
2. Isabaev B. Mezhdunarodno-pravovoj uroven obespecheniya informatsionnoj bezopasnosti // Vestnik KazNU. 2011. 234 s.
3. Zinoveva E. S. Mezhdunarodnaya informatsionnaya bezopasnost. M.: MGIMO-Universitet, 2013. S. 118-123.
4. Kapustin A.Ya. Ugrozy mezhdunarodnoj informatsionnoj bezopasnosti: formirovanie kontseptualnykh podkhodov // Zhurnal rossijskogo prava. 2015. № 8. S. 89-100.
5. Krylov G. O. Mezhdunarodnyj opyt pravovogo regulirovaniya informatsionnogo regulirovaniya Rossijskoj Federatsii: Avtoref. diss. … kand. yurid. nauk. M., 2007. S. 6-7.
6. Krutskikh A. V., Streltsov A. A. Mezhdunarodnoe pravo i problema obespecheniya mezhdunarodnoj informatsionnoj bezopasnosti // Mezhdunarodnaya zhizn. 2014. № 11.
7. Markov A. Nekotorye aspekty informatsionnoj bezopasnosti v kontekste natsionalnoj bezopasnosti // Vestnik SPbGU. Ser. 12. Vyp. 1. S. 43-48.
8. Morozova A. V., Polyakova T. A. Organizatsionno-pravovoe obespechenie informatsionnoj bezopasnosti. M.: RPA Minyusta Rossii, 2013. 276 s.
9. Pelevina E. S. Osobennosti sistemy informatsionnoj bezopasnosti kak elementa mezhdunarodnoj bezopasnosti v sovremennom mire // Teorii i problemy politicheskikh issledovanij. 2017. T. 6. № 1A. S. 194-205.
10. Radysh M. Belaya kniga rossijskikh spetssluzhb. M.: Obozrevatel. 2016. S. 113.
11. Smirnov A. I. Rossijsko-amerikanskoe sotrudnichestvo v oblasti mezhdunarodnoj informatsionnoj bezopasnosti: predlozheniya po prioritetnym napravleniyam // Mezhdunarodnaya zhizn. 2017. № 11. S. 72-81.
12. Strategicheskij vektor obespecheniya mezhdunarodnoj informatsionnoj bezopasnosti. SPb.: SPII RAN, 2016. 122 s.