УДК 342.951:351.82

И. П. Михнев
Волгоградский институт управления (филиал) ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ», Волгоград, e-mail: mkmco@list.ru

С. В. Михнева
Волгоградский институт управления (филиал) ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ», Волгоград, e-mail: svet-mihneva@list.ru

А. Г. Айвазян
Волгоградский институт управления (филиал) ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ», Волгоград, e-mail: ayyvazyan.angela@gmail.com

Е. П. Серкина
Волгоградский институт управления (филиал) ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ», Волгоград, e-mail: serkina.elizaveta1@gmail.com

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ДОСТИЖЕНИЯ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Ключевые слова: правовое регулирование, информационная безопасность, защита информации, угрозы информационной безопасности, критическая информационная инфраструктура, компьютерный инцидент, субъекты критической информационной инфраструктуры.

В работе рассматриваются правовые основы сферы информационной безопасности, которую сегодня следует отличать от форм, процедур и процессов защиты информации. В Российской Федерации сегодня действуют два основных федеральных закона, закрепляющие и формулирующие основные понятия в области информационной безопасности. Проанализированы основные положения нового вступившего в силу с 1 января 2018 года Федерального закона №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Сделаны выводы о том, что ускорение темпов развития общественных отношений, информационных процессов диктует принятие и внедрение современных необходимых процедур модернизации способов защиты информации, что закономерно предполагает развитие и совершенствование действующей законодательной базы. В связи с чем, сегодня законодательно введены и внедряются на практике новые элементы механизма обеспечения безопасности критической информационной инфраструктуры, такие как, объекты такой инфраструктуры, компьютерная атака и инцидент. Выделены показатели критериев значимости объектов критической информационной инфраструктуры. А также создан национальный координационный центр по компьютерным инцидентам и определен ряд полномочий Президента РФ, иных органов федеральной государственной власти в сфере обеспечения информационной безопасности.

Введение

Национальная безопасность любого государства как состояние защищенности от внешних и внутренних угроз, атак, террористических актов и иных противоправных, незаконных операций и воздействий охватывает различные всевозможные сферы общественной жизнедеятельности. Так, можно выделить политическую, экономическую, территориальную, геополитическую, правовую составляющие национальной безопасности. При этом, одной из важнейших является безопасность в сфере информационного поля, пространства, информационных ресурсов и информационных систем. Таким образом, информационная безопасность представляет собой наиболее актуальную сегодня область и составляющую национальной безопасности, поскольку любая иная система строится на передаче, сохранении и обработке ценной и важной, в той или иной степени секретной конфиденциальной информации, необходимой для обеспечения государственной безопасности и предотвращения национальных угроз [1].

Современные демократические страны осуществляют правовую и информационную политику, направленную на построение и развитие правового государства, в котором строго и неукоснительно соблюдается принцип приоритета прав и свобод человека и гражданина, их защита и охрана. Правовая и информационная системы общества, включающие в себя как субъекты права и информационного поля, так и формы их юридического, технического, информационного, технологического, организационно-коммуникативного взаимодействия, активно развиваются в сторону информатизации, что необходимо в целях усовершенствования юридического процесса, оптимизации документооборота [2].

Однако, сегодня как относительно новая и потому еще только развивающаяся сфера современной государственно-правовой действительности информационное пространство не достаточно полно и оптимально урегулировано правовыми нормами. Нужды и вызовы современной жизни выдвигают ряд требований к законодателю, направленных на повышение эффективности и устранение юридических неточностей, коллизий и пробелов в сфере защиты информации. И как следствие, незаконное и (или) случайное распространение информации, носящей строго конфиденциальный характер, вызванное неправомерными действиями сотрудников организаций, учреждений и предприятий проводит к неточному исполнению должностных профессиональных обязанностей и полномочий, подрывает авторитет власти.

Современная геополитическая ситуация в мире, обусловленная борьбой с террористическими угрозами, нарушающими безопасность людей и, в целом, государств, противоречащими правам человека, диктует принятие своевременных мер, в том числе, по защите информационных ресурсов, систем и обеспечению информационной безопасности. В тоже время обострение конфликтов и столкновение экономических, политических и территориальных интересов различных государств не способствует эффективному взаимному межгосударственному сотрудничеству в разных направлениях, успешному обмену информационными данными и показателями. В связи с чем, все чаще сегодня приходит слышать понятие – информационная война, которое прочно входит в международный оборот и диктует свои правила игры и условия государственных отношений.

Информационные отношения сегодня являются предметом современного информационного права и законодательства, хотя уже к концу 20 века в России сформировались начала юридической науки информационного права. В Российской Федерации самостоятельного закона об информационной безопасности на сегодняшний день не принято. Однако нормы и положения, так или иначе затрагивающие проблему защиты информации и обеспечение информационной безопасности, содержатся в Федеральном законе 2006 года «Об информации, информационных технологиях и о защите информации» [3], в утвержденной 5 декабря 2016 году Президентом Российской Федерации Доктрине информационной безопасности [4] и Указе Президента Российской Федерации от 20 января 1994 г. №170 «Об основах государственной политики в сфере информатизации» [5]. Серьезной новеллой, подчеркивающей актуальность рассматриваемых вопросов в связи с относительно недавними событиями в других государствах и безосновательными обвинениями, выдвигаемых в сторону России, стало принятие в 2017 году нового Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», который вступил в силу с 1 января 2018 года [6]. Таким образом, анализ нормативных установлений в этой сфере и их соответствие реалиям современности позволит выявить степень эффективности правового регулирования и уязвимые места информационных защитных систем.

Цель исследования – используя выработанный в науке широкий спектр подходов и концепций, а также опираясь на нормы и положения действующего законодательства, проанализировать правовое регулирование информационной безопасности в Российской Федерации.

Материалы и методы исследования

Нормативно-правовую базу исследования составляют следующие официальные акты: Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26 июля 2017 года №187-ФЗ

«О безопасности критической информационной инфраструктуры Российской Федерации», Указ Президента Российской Федерации от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации», Указ Президента РФ от 22.12.2017 года № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», Постановление Правительства Российской Федерации от 17.02.2018 года № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Методологическую основу составили диалектический метод научного познания объективной действительности, а также основанные на нем общенаучные и частнонаучные методы, прежде всего, социологический, статистический, сравнительно-правовой, конкретно-исторический, структурно-функциональный, формально-юридический, основные общелогические методы познания (анализ, синтез, индукция, дедукция). Использовались методы системного изучения объекта исследования в его внутренних и внешних взаимосвязях, в историческом развитии.

Данная тема, посвященная анализу правового регулирования информационной безопасности и деятельности по ее обеспечению, находится на стыке различных отраслей права и разных наук. С одной стороны, такие юридические отраслевые науки как: конституционное право, закрепляющее общие положения сферы безопасности и защиты информации; информационное право, непосредственное имеющее предметом правового регулирования информационные отношения; административное и уголовное право, предусматривающие наказания за противоправные действия в информационной сфере.

С другой стороны, одной лишь юриспруденции недостаточно для всестороннего охвата правовой регламентации информационной безопасности ввиду технической составляющей данного явления. В связи с чем, такие точные науки, как физика (физические каналы связи) и математика (криптография) позволяют выделить основные технологические позиции и приоритеты, требующие непосредственной защиты информации и, как следствие, их правовой регламентации. Например, такие способы защиты как резервное копирование во избежание случаев похищения персональной информации, поскольку не только компьютеры подвергаются непосредственному вредоносному хакерскому воздействию, но и другие устройства могут быть объектом атак как носители информации и ее обработки. Проблемой дня сегодня является «скрытый майнинг», т. е. возможность незаконной добычи злоумышленниками криптовалюты посредством использования факта посещения любым субъектом определенных страниц. Поэтому авторы криптомайнеров используют огромный масштаб возможностей проникновения в чужие сети. Эффективное выявление майнеров сегодня самая актуальная задача современной информационной безопасности [7].

К сожалению, скорость, с которой развиваются как информационные технологии, так и способы хакерских атак на них и методы вредоносных действий на оперативные системы, намного выше скорости изменения нормативно-правовой базы в этой области. Однако, принятие в 2017 году нового федерального закона о безопасности критической информационной инфраструктуры явилось ответом на обострение ситуации в сфере защиты информации общегосударственного масштаба. В связи с чем, законодатель четко обозначил субъектов – обладателей критической информационной инфраструктуры, определил и закрепил их правовой статус в виде совокупности прав и обязанностей [8].

Актуальность и восстребованность информационных потоков и обеспечение их безопасности позволяет определить с позиции юридической науки в системе права нового структурного элемента – правового обеспечения информационной безопасности. Он обусловлен научно-техническим прогрессом, развитием информационных технологий, возрастанием экономической, социальной значимости информации, развитием информационного общества и возникновением угроз интересам его субъектов, необходимостью охраны социально значимых ценностей в информационной сфере и совершенствования законодательства об информационной безопасности.

Информационные потоки охватывают все сферы общественной жизнедеятельности. Управление информационными потоками должно осуществляться на уровне государственной власти, органы которой осуществляют управление информатизацией общества и контроль за этой деятельностью. В связи с чем, важное значение уделяется информационной безопасности в сфере государственного управления.

Следует отметить, что законодательные основы любого государства в области информационной безопасности являются необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических, геополитических, военных и иных направлений функционирования этого государства. Сегодня информационная безопасность становится базовым элементом системы национальной безопасности России, что обусловлено быстро растущими технологическими возможностями современных информационных систем, влияющих на хозяйственно-экономическую жизнь, духовно-идеологическую сферу и умонастроения людей [9].

Нормативная база по вопросам информационной безопасности России включает Конституцию Российской Федерации, федеральные законы; кодексы Российской Федерации; постановления Правительства Российской Федерации; ведомственные нормативные акты. Правовой основой обеспечения информационной безопасности является Федеральный закон от 27.07.2006 г. №149-ФЗ (в редакции от 19.07.2018 г.) «Об информации, информационных технологиях и о защите информации». Важным документом является Указ Президента РФ от 20 января 1994 г. №170 «Об основах государственной политики в сфере информатизации». Основополагающим документом в области информационной безопасности является утвержденная 09.09.2000 г. Президентом Российской Федерации Доктрина информационной безопасности, представляющая совокупность целей, задач, принципов, основных направлений обеспечения информационной безопасности Российской Федерации. Доктрина служит основой для формирования государственной политики в области обеспечения информационной безопасности Российской Федерации, подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации, разработки целевых программ обеспечения информационной безопасности Российской Федерации [10]. Таким образом, непосредственно нормативно-правового акта о правовых основах, формах и методах информационной безопасности сегодня не принято. Однако, несколько компенсировалась ситуация в связи с принятием в 2017 году и вступлением в силу в 2018 году нового федерального закона о безопасности критической информационной инфраструктуры России.

В связи с чем, анализ правовых основ в этой деятельности должен опираться на положения ныне действующего законодательства. Необходимость принятия официального законодательного документа об информационной безопасности продиктована современными угрозами информационным ресурсам. Поэтому, учитывая сформированные в России органы государственной власти и местного самоуправления требуется предусмотреть информационную безопасность как для физических лиц и частных юридических лиц, а также для органов власти – публично-правовых субъектов права.

В соответствии с Указом Президента Российской Федерации от 20 января 1994 г. №170 «Об основах государственной политики в сфере информатизации» установлено, что реализация государственной политики в сфере информатизации обеспечивается системой государственных органов, включающей органы управления при Президенте Российской Федерации, федеральные и региональные органы исполнительной власти [11]. В соответствии с российским действующим законодательством государственное регулирование в сфере применения информационных технологий предусматривает развитие информационных систем различного назначения для обеспечения граждан, организаций, органов государственной власти и местного самоуправления информацией, а также обеспечение взаимодействия таких систем.

Результаты исследования и их обсуждение

Понятие «информационная безопасность» включает в себя множество

компонентов, процессов, форм, условий, процедур различных наук, как, прежде всего, технических и физико-математических, так и социальных, и юридических. Непосредственно информационная безопасность всех участвующих в информационном поле субъектов обеспечивается техническими, технологическими и информационно-физическими методами, средствами и способами защиты сведений. Однако, осуществляясь в границах только каждой конкретной организации частноправового или публично-правового характера, приоритеты политики безопасности в информационной сфере служб IT могут определяться основными направлениями деятельности организации, ее организационно-правовой формой и правовым положением. Но общегосударственный уровень информационной безопасности концептуально должен определять систему мер, направленных на защиту информации. В юридическом смысле информационная безопасность является комплексным правовым институтом, поскольку определяется с позиции различных отраслей права [12].

Федеральным законом №149-ФЗ об информации и ее защите определены обязанности обладателя информации, которые сводятся в основном к следующему: предотвращение несанкционированного доступа к информации, своевременное обнаружение фактов несанкционированного доступа к информации, предупреждение возможности неблагоприятных последствий нарушения порядка доступа к сведениям, недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование, возможность незамедлительного восстановления информации, поврежденной или ликвидированной по причине несанкционированного доступа к ней, перманентный контроль и надзор за обеспечением необходимой защиты информации.

Информационная безопасность в соответствии с Федеральным законом 1996 г. №85-ФЗ «Об участии в международном информационном обмене» – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства. На базе этого определения ученые сформулировали такое понятии информационной безопасности как состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности [13]. Цель информационной безопасности – защита информации и прав субъектов информационной деятельности при формировании информационных технологий, инфраструктуры и информационных ресурсов путем проведения правовых, организационных и технических мероприятий. Объектом информационной безопасности рассматривается информация, затрагивающая государственные, служебные, коммерческие, интеллектуальные и личностные интересы, а также это – средства и инфраструктура ее обработки и передачи. Информационная безопасность касается государственных информационных ресурсов. Важность их сохранения обусловлена тем, что это информация, которая содержится в государственных информационных системах, а также различного рода сведения и документы, имеющиеся в распоряжении государственных органов [14].

Информационная безопасность, как и в целом, национальная строится на принципах законности, демократизма, плюрализма, повышенной юридической ответственности должных лиц государственной власти и местного самоуправления, профессионализме и ответственности государственных и муниципальных служащих, приоритета прав и свобод человека и гражданина, приоритета национальных интересов, активном участии граждан в повышении информационной грамотности и культуры и других. Информационную безопасность следует отличать от защиты информации, несмотря на смысловую схожесть двух терминов. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, от иных неправомерных действий в отношении такой информации, соблюдение конфиденциальности информации ограниченного доступа, реализацию права на доступ к информации [15].

Информационная безопасность ранее представляла процедуры аутентификации, авторизации и криптографии. С появлением компьютерных вирусов повысились угрозы, хакерские атаки и другие способы

неправомерного и несанкционированного вмешательства и воздействия на операционные системы. Борьба в первоначальных стадиях обеспечения безопасности показала низкий уровень защитных мероприятий. Вредоносные программы стали угрожать приватности, похищая ценную информацию и сведения, представляющие определенного рода тайну. В связи с чем, новый федеральный закон №187-ФЗ регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры России именно в целях ее устойчивого функционирования в случае возникновения и проведения в отношении ее компьютерных атак. Он позволяет государственным органам, Центральному Банку России и государственным организациям устанавливать и утверждать дополнительные требования по обеспечению безопасности значимых объектов критической инфраструктуры [16].

Объектами критической информационной инфраструктуры в соответствии с законом являются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, которые предусмотрены специальным реестром. Субъектами являются государственные органы и учреждения, юридические лица РФ, индивидуальные предприниматели, которые на законном основании владеют информационными системами. Поэтому они обязаны информировать представителей власти о компьютерных инцидентах, предотвращать неправомерные попытки доступа к информации и обеспечивать возможность восстановления функционирования объекта за счет создания резервных копий документов, данных, иных видов сведений и другой информации [17]. Максимальные санкции за создание вредоносных программ для кибератак на критическую информационную инфраструктуру предусматривают до 10 лет лишения свободы.

Выводы (заключение)

Современные закономерности и тенденции широкомасштабного ускоряющегося процесса развития и при этом совершенствования информационных систем и технологий наглядно демонстрируют возрастание актуальности проблемы поиска высокого уровня технических, юридических, организационных и иных мероприятий обеспечения информационной безопасности в сегодняшних условиях, когда множество внедряющихся компьютерных вирусов и информационные войны угрожают национальной безопасности нашего государства. Таким образом, актуальность обеспечения на государственном уровне информационной безопасности на сегодняшний день очевидна, так как напрямую связана с сохранением государственной целостности и безопасности в целом. Безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак (ст. 2 ФЗ №187). Новизна в том, что введены впервые новые понятия, в частности, критическая информационная инфраструктура, компьютерная атака как целенаправленное воздействие программных или программно-аппаратных средств на объекты критической информационной инфраструктуры для их нарушения, компьютерный инцидент, выражающийся в факте нарушения или прекращения функционирования объекта критической информационной инфраструктуры. Впервые появляется новый принцип обеспечения безопасности – приоритет предотвращения компьютерных атак, а также создана государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак. Определены полномочия Президента РФ и органов государственной власти в сфере обеспечения безопасности критической информационной инфраструктуры. Впервые выделены показатели критериев значимости объектов критической информационной инфраструктуры, предполагается создание национального координационного центра по компьютерным инцидентам.

Развитие информационных систем по всему миру идет с ускоряющейся динамикой. Руководители государств объективно и научно подходят к вопросу о создании актуального эффективного механизма защиты информации. Однако, и сегодня мы наблюдаем ситуацию, когда частные физические лица могут без особых усилий взломать систему охраны банковских организаций или становимся свидетелями «подрывной» деятельности так называемых хакеров в органах государственной власти.

Обеспечение информационной безопасности предполагает объединение совместных усилий на всех уровнях власти: федеральном, региональном и на муниципальном уровне. На корпоративном уровне сами организации, заинтересованные в достаточно эффективной системе информационной безопасности и защите своих информационных интересов, информационных потоков и документальных, фактологических сведений, должны предусмотреть необходимые технические, юридические, программные ресурсы, позволяющие наладить механизм защиты информации в целях обеспечения информационной безопасности конкретного предприятия. Поэтому на внутриорганизационном уровне комплекс мер, направленных на защиту информации и обеспечение безопасности, определяется значимостью получаемой, обрабатываемой и хранимой информации.

Библиографический список

1. Михнев И.П., Сальникова Н.А., Кравец А.Г. Защита информации от несанкционированного доступа при анализе радиационных характеристик помещений спектрометрическим методом // Известия Волгоградского государственного технического университета. – 2018. – № 8 (218). – С. 105–109.

2. Митячкина Е.С., Михнева С.В. Правовое регулирование положения главы местной администрации и муниципального служащего в Российской Федерации // Гуманитарные исследования. – 2016. – № 2 (58). – С. 157–162.

3. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета – Федеральный выпуск № 4131 (0), 29 июля 2006 г.

4. Доктрина информационной безопасности РФ (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) // Собрание законодательства РФ. – 12.12.2016. – № 50. – Ст. 7074.

5. Указ Президента РФ от 20 января 1994 г. № 170 «Об основах государственной политики в сфере информатизации» (с изменениями и дополнениями от 9 июля 1997 г.) // Российская газета – Федеральный выпуск № 1233 (132), 12 июля 1997 г.

6. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета – Федеральный выпуск. – № 7333 (167). – 31 июля 2017 г.

7. Михнева А.И. Формирование местного самоуправления в Российской Федерации: организационно-правовые аспекты // Аллея науки. – 2018. – Т. 5, № 4 (20). – С. 813–817.

8. Сальникова Н.А., Михнев И.П. Проведение аттестации знаний студентов с помощью компьютерного тестирования // Известия Волгоградского государственного технического университета. Серия: Новые образовательные системы и технологии обучения в вузе. – 2007. – Т. 4, № 7 (33). – С. 182–184.

9. Михнев И.П., Михнева С.В. Природные радионуклиды как источник фонового облучения населения Нижневолжского региона // Образование и наука: современные тренды. Коллективная монография. Сер. «Научно-методическая библиотека» / гл. ред. О.Н Широков. – Чебоксары, 2018. – С. 151–166.

10. Михнева С.В., Михнев И.П., Чернова А.П. Правовые основы определения юридического положения должностных лиц местного самоуправления и муниципальных служащих в Российской Федерации // Социально-экономические и правовые основы инновационного развития: сборник научных статей. – Пенза, 2018. – С. 104–111.

11. Михнев И.П., Сальникова Н.А., Мединцева И.П. Защита конфиденциальной информации от несанкционированного доступа при проектировании автоматизированных систем радионуклидной спектрометрии на базе сцинтилляционного гамма-спектрометра // Научное обозрение: коллективная монография / гл. ред. Э.Н. Рябинина. – Чебоксары, 2018. – С. 48–58.

12. Кленина В.И. Информационные технологии в профессиональной деятельности юриста // Ученые записки. – 2010. – № 7. – С. 99–102.

13. Михнева С.В., Митячкина Е.С. Ценностные характеристики местного самоуправления // Гуманитарные исследования. – 2017. – № 4 (64). – С. 248-253.

14. Краткий обзор ИТ-технологий, используемых в юридической деятельности / Р.Г. Драпезо и др. // Вестник Кемеровского государственного университета. – 2013. – № 1(53). – С. 306–312.

15. Михнева С.В., Сорокина Н.В. Образование и профессиональная подготовка муниципальных служащих как факторы демократического развития Российской Федерации // Профессиональные инновации. – 2013. – № 4. – С. 97.

16. Бачолин Н.Л. Информационное право. Основы практической информатики. – М.: Юринформцентр, 2012.

17. Маруков А.Н. Компьютерные преступления: классификация и способы противодействия: учебное пособие. – М.: Логос, 2015.