УДК 343

ИСТОРИЯ РАЗВИТИЯ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

А.В. Поваляева, В.В. Мирончуковская
Елецкий государственный университет им. И.А. Бунина
(Елец, Россия)

Аннотация. *В статье рассматриваются вопросы развития уголовного законодательства в сфере обеспечения национальной безопасности в России в исторической ретроспективе. Исследуются различные подходы ученых начала XX века в определении объекта преступления. Анализируются отдельные нормативно-правовые акты советского периода об обеспечении информационной безопасности государства. Выделяются ключевые этапы реформирования государственных органов в сфере обеспечения информационной безопасности и их последствия.*

Выделяется как самостоятельный объект – информационная безопасность. Отмечается отсутствие комплексного подхода в законодательстве к решению вопросов обеспечения информационной безопасности.

Подчеркивается важная роль нормативно-правовых актов XXI века – международных и национальных, которые устанавливают правовые основы обеспечения информационной безопасности.

Информационная безопасность, взяв на себя контроль за системой общественных отношений, является еще и составляющей информационного права, как одного из институтов России. Поэтому грамотное обеспечение защиты информационной безопасности уголовно-правовыми средствами очень важно.

Обратившись к современному законодательству можно увидеть, что как таковая система обеспечения защиты информационной безопасности там отсутствует. То есть, по сути, в Уголовном кодексе Российской Федерации нет конкретной главы или раздела, который посвящался бы только информационной безопасности. Все пункты, имеющие отношение к этому понятию разбросаны по разным главам.

Авторы делают вывод, что информационные ресурсы составляют основу духовного и научно-технического потенциала России. Поэтому их необходимо использовать рационально и сохранять, не нарушая при этом конституционные права граждан, обеспечив им свободный доступ к получению, передаче, поиску и распространению информации законными способами.

Ключевые слова: *информационная безопасность, преступление, национальные интересы, информационные технологии*

DOI 10.24888/2949-3293-2024-4-4-56-67

THE HISTORY OF THE DEVELOPMENT OF CRIMINAL LAW IN THE FIELD OF INFORMATION SECURITY IN RUSSIA

Alina V. Povalyaeva, Victoria V. Mironchukovskaya
Bunin Yelets State University
(Yelets, Russia)

Abstract. *The article examines the development of criminal legislation in the field of national security in Russia in historical retrospect. Various approaches of scientists from the beginning of the XX century in determining the object of the crime are being studied. Separate normative legal acts of the Soviet period on ensuring the information security of the state are analyzed. The key stages of reforming state bodies in the field of information security and their consequences are highlighted.*

It stands out as an independent object – information security. The lack of an integrated approach in legislation to addressing issues of information security is noted.

The important role of normative legal acts of the XXI century is emphasized – international and national, which establish the legal basis for ensuring information security.

Information security, having assumed control over the system of public relations, is also a component of information law, as one of the institutions of Russia. Therefore, competent provision of information security protection by criminal law means is very important.

Turning to modern legislation, one can see that there is no information security protection system as such. That is, in fact, there is no specific chapter or section in the Criminal Code of the Russian Federation that would be devoted only to information security. All the items related to this concept are scattered in different chapters.

The authors conclude that information resources form the basis of the intellectual and scientific and technical potential of Russia. Therefore, they must be used rationally and preserved without violating the constitutional rights of citizens, providing them with free access to receive, transmit, search and disseminate information in any way.

Keywords: *information security, crime, national interests, information technology*

Информационная безопасность, относительно уголовного права, является системой общественных отношений, охраняемых законом. Это связано с научным обоснованием объекта преступления уголовного права, которым и являются те же самые общественные отношения. Однако это мнение разделяется не всеми учеными.

Так, еще до наступления революции в России существовало несколько интерпретаций объекта преступления. Большинство этих идей были основаны на мнении немецкого криминалиста А. Фейербаха, который определял объект как субъективное право.

Например, В.Д. Спасович определял преступление как «посягательства на чьелибо право, охраняемое государством посредством наказания». Из этого мнения следовало, что предметом преступления обязательно будет только лицо и, если государство отменит защиту права, то его нарушение уже не будет уголовно наказуемым [13, с. 94]. Позже В.Д. Спасович разработал теорию нормативного права, которое получило известность в России в начале 19 века.

Критиком указанных выше теорий выступал С.В. Познышев, который рассматривал свое видение объекта преступления, как конкретных отношений, состояний лиц или вещей, охраняемых законом под страхом наказания [12, с. 133]. Похожее мнение высказывал Н.С. Тагинцев, который видел объект преступления не только как юридическую норму, но и как стоящие за ней блага и интересы.

В науке отечественного уголовного права понятие объекта преступления как общественных отношений появилось только в 1924 году, благодаря публикации его в одном из учебников уголовного права А.А. Пионтковским. Эта идея легла в основу современного законодательства.

Информационная безопасность, взяв на себя контроль за системой общественных отношений, является еще и составляющей информационного права, как одного из институтов России. Поэтому грамотное обеспечение защиты информационной безопасности уголовно-правовыми средствами очень важно.

Обратившись к современному законодательству, можно увидеть, что как таковая система обеспечения защиты информационной безопасности там отсутствует. То есть, по сути, в Уголовном кодексе Российской Федерации нет конкретной главы или раздела, который посвящался бы только информационной безопасности. Все пункты, имеющие отношение к этому понятию, разбросаны по разным главам. Поэтому хотелось бы рассмотреть, каким образом строилось законодательство в России в отношении защиты информационной безопасности.

Для начала следует отметить, что информационные технологии были известны миру еще со времен СССР, но отечественная политика долго не строилась на информационном обществе, в отличие от других прогрессивных стран. Наиболее важными периодами в построении технологий были 70-е и 80-е годы. Еще с начала 70-х годов активно использовались технические средства разведки, а в 80-е начался бурный научно-технический прогресс в области военного производства. Хотя довольно длительное время Советский Союз старался сдержать натиск западных стран в информационной войне, но, в конце концов, потерпел поражение. Однако в дальнейшем, после распада СССР, страна сохранила значительную часть технологической системы бывшего Союза, что дало право на обеспечение защиты внутренней информационной сферы.

Но мы углубимся еще дальше в 20-е годы, где проявили себя первые зачатки системы информационной безопасности. Все началось с постановления Малого Совнаркома от 5 мая 1921 года при ВЧК о создании специального отдела под руководством Г.И. Бокия. Это была первая криптографическая служба, к которой позже присоединились и эксперты дешифровальщики.

В октябре того же года Декретом СНК утверждается список сведений, которые не подлежат распространению и составляют военную или экономическую тайну. Следом, постановлением СНК РСФСР от 13 октября 1921 года создается «Положение о военной цензуре ВЧК», в котором указывается цензура печатных изданий, произведений, корреспонденций и вводится контроль над радиотелеграфными связями, в целях защиты военных, экономических и политических интересов. В июне 1922 года образовывается Главное управление по делам издательства при Наркомате просвещения, которое контролирует издательскую деятельность.

Стоит упомянуть и первый советский уголовный кодекс, который был принят в мае 1922 года и собрал в себе нормативные акты и судебные практики, использовавши-

еся ранее. В дальнейшем он не раз будет подвергаться изменениям в соответствии в политической обстановкой того или иного периода.

В августе 1922 года Секретариат ЦК РКП (б) принимает постановление «О порядке хранения и движения секретных документов». Они же и утверждают постановление «О порядке хранения секретных постановлений ЦК РКП (б)» [5, с. 55]. При этом для хранения секретных документов выделяются специальные секретные части.

За период 30-х годов стоит отметить три приказа и одно постановление. Это Приказы НКО СССР от 1930 года о «Наставлении по мобилизационной работе в войсковых частях, управлениях, учреждениях и заведениях РККА», от 1937 года «Положение о центральной военной цензуре РУ» и от 1939 года о «Наставлении по секретному делопроизводству в РККА». Постановление СНК СССР было утверждено 17 июня 1939 года и называлось «О реорганизации фельдъегерской связи НКВД СССР», где перевозка секретных писем возлагалась на фельдъегерскую связь НКВД и специальную связь Наркомата связи [5, с. 67].

В 1947 году вновь расширяется список секретных сведений с выходом постановления СМ СССР «Об установлении перечня сведений, составляющих государственную тайну, разглашение которых карается по закону». Затем, Указом Президиума Верховного Совета СССР утверждается документ под названием «Об ответственности за разглашение государственной тайны и за утрату документов, содержащих государственную тайну», где были указаны санкции за несоблюдение первого постановления. В том же году был создан Комитет информации, занимавшийся вопросами внешней разведки, который просуществовал всего четыре года, после чего его функции были вновь отданы под управление МГБ СССР.

В марте 1948 года постановлением Совета Министров СССР выходят «Перечень главнейших сведений, составляющих государственную тайну» и «Инструкция по обеспечению сохранности государственной тайны в учреждениях и на предприятиях СССР». В перечне сведения подразделялись на 8 позиций, где были отражены мобилизационные вопросы, финансовые, политические, экономические, военные, научно-технические, информация об Арктике и другие сведения. Инструкция определяла порядок секретности сведений с указанием ее степени (всего их было три) и классифицировала названия секретных органов.

50-е годы ознаменованы большим количеством законодательных реформ и разнообразием реорганизаций. Так вначале 50-х годов все еще функционирует МГБ СССР, а уже в 1953 году, после смерти Сталина, оно входит в состав МВД СССР. В 1954 году при СМ СССР создается Комитет государственной безопасности (КГБ), за счет чего усиливаются органы государственной безопасности. В каждой военной отрасли образовываются особые отделы КГБ, т.е. органы военной контрразведки [10, с. 504]. В конце 50-х утверждается Положение о КГБ при СМ СССР и его органах на местах, где прописываются его основные задачи, такие как контрразведывательная и разведывательная работа на разного рода секретных объектах, борьба со шпионской деятельностью внутри СССР, охрана государственных лиц и границ, организация правительственной связи, разработка нормативных актов, инструкций, положений и планов, связанных с разведывательной деятельностью.

В тот же период особо уделяется внимание вопросам защиты связи. В 1958 году создается Центральная межведомственная комиссия по электросвязи, которая занима-

лась пресечением подслушиваний на государственных границах, перевозкой секретных сведений и техники посредством спецсвязи и фельдсвязи, разработкой мероприятий для улучшения защиты связи. Выходит постановление ЦК КПСС «О мерах по сохранению государственной тайны».

В феврале 1960 года произошла очередная реорганизация. На этот раз была сокращена численность КГБ и изменена их структура. А в 1967 году в районах и городах были реорганизованы аппараты уполномоченных в соответствующие отделы и отделения КГБ. В июле того же года ЦК КПСС и СМ СССР дают возможность КГБ самостоятельно организовать подразделения по борьбе с идеологической диверсией противника на местах [5, с. 102].

В 60-е годы происходит расширение состава органов, выполняющих вышестоящие функции защиты государственных секретов. К таким органам относились, например, ГКГБ, ГК СССР по технике и науке, Главное управление картографии и геодезии и по охране гостайн и печати.

Относительно 60-х годов следует упомянуть и изменения уголовного законодательства по отношению к национальной безопасности. Так, Президиумом ВС СССР были внесены дополнения. Это послабление мер в виде освобождения от ответственности граждан СССР, которые были завербованы иностранной разведкой, если они делали добровольное признание и не совершили никаких противоправных действий; установление срока заключения 7 лет с последующей 5-летней ссылкой за распространение агитационной информации с целью подрыва власти. В 1966 году ВС СССР принимают указ «Об уголовной ответственности иностранцев и лиц без гражданства за злостные нарушения правил движения по территории СССР». Годом позже СМ СССР подписывается постановление «Об упорядочении системы ознакомления иностранных делегаций, отдельных ученых и туристов с научно-техническим достоянием СССР», в котором рассматривался порядок приема иностранных делегаций. Так, согласно постановлению, руководители предприятий, которые хотят принять иностранных гостей, должны были обязательно согласовать это мероприятие с органами государственной безопасности за 5 дней до приема, составить и утвердить план приема, выбрать заранее объекты и предметы показа, организовать специальные помещения вне охраняемых зон, в случае регулярного приема иностранцев, фиксировать информацию с результатами этих встреч.

В 1973 году ЦК КПС и СМ СССР принимают постановление «О мерах противодействия иностранным техническим разведкам», благодаря которому разрабатываются новые способы противодействия иностранной разведке по отношению к военной промышленности под управлением Государственной комиссии СССР по противодействию иностранным техническим разведкам.

Годом ранее Указом Президиума ВС СССР выходит документ под названием «О применении органами государственной безопасности предостережения в качестве меры профилактического воздействия» [15, с. 155]. Благодаря ему органы государственной безопасности могли делать официальные предупреждения в виде протоколов гражданам, которые не совершали уголовного деяния, но, например, допускали контакты с иностранцами или нарушали правила обращения с документацией.

В 1976 году ЦК КПСС и СМ СССР выпускают постановление «О мерах по дальнейшему совершенствованию системы сохранения государственных секретов». В

том же году хочется отметить и принятие постановления «О мерах противодействия иностранным техническим разведкам», которое было выпущено для развития постановления «О мерах по усилению режима секретности», принятое шестью годами ранее.

7 октября 1977 года в силу вступила новая Конституция СССР, где обеспечение информационной безопасности государства выносилось на первый план и отдавалось под контроль высших органов государственного управления и власти СССР [5, с. 113]. Это нововведение имело большое значение для совершенствования деятельности органов защиты информации.

С конца 70-х и вначале 80-х годов происходят значительные изменения в структуре КГБ. В 1978 году их переименовывают из КГБ при Совете Министров СССР в КГБ СССР. В сентябре 1981 года внутри КГБ создается самостоятельное 4-е Управление, занимающееся контрразведкой на объектах транспорта и связи. В 1982 году подобно создается 6-е Управление по защите экономики от действий иностранных спецслужб. В 1983 году в КГБ образуется специальное подразделение по защите ОМВД СССР. Затем реорганизация КГБ происходит в основном в связи с демократизацией общественной жизни в СССР [6, с. 45].

В 1984 году вышел Указ Президиума ВС СССР «О внесении изменений и дополнений в некоторые законодательные акты СССР об уголовной ответственности и уголовном судопроизводстве», которым устанавливалась уголовная ответственность за передачу научно-технических, экономических и других секретных сведений иностранным организациям лицами, которым эта информация была доверена по службе [14, с. 367]. Так как военное производство в этот период развивалось полным ходом, вопросы защиты информации стояли особенно остро и подобные нововведения были необходимы.

90-е годы в истории России считаются наиболее неоднозначными и разнообразными, как по части развития, так и по части распада. Это время активного развития предпринимательства, появления мобильных телефонов, компьютеров и Интернета. С другой стороны этот период характеризуется распадом экономики, политическим кризисом, развалом СССР и ростом терроризма. Также в это время происходит большое количество законодательных изменений.

С наступлением технического прогресса вопрос обеспечения информационной безопасности становится все важнее. Еще до распада СССР в 1990 году Главное управление по охране государственных тайн в печати при Совете Министров СССР утверждает «Методические рекомендации по охране сведений, подлежащих защите от разглашения в печати и других средствах массовой информации». В этом же году СМ СССР утверждает «Положение о разработке, изготовлении и обеспечении эксплуатации шифровальной техники, государственных и ведомственных систем связи и управления и комплексов вооружения, использующих шифровальную технику».

16 мая 1991 года ВС СССР принимают закон «Об органах государственной безопасности в СССР», который давал контроль высшим органам государственной власти и прокуратуре следить за исполнением своих обязанностей органам государственной безопасности. В августе 1991 года происходит распад СССР и возникновение СНГ, после чего последний закон утрачивает силу [11, с. 116].

Далее в части защиты информации нормативный акт появляется только в апреле 1994 года. Это было «Положение о государственном лицензировании деятельности в

области защиты информации», утвержденное совместным решением Государственной технической комиссии при Президенте РФ и Федерального агентства правительственной связи и информации при Президенте РФ. В этом же году постановлением Правительства РФ утверждается «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

В 1995 году постановлением Правительства выходят еще 3 документа. Это «Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», «Положение о сертификации средств защиты информации» и «Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности». В ноябре того же года Указом Президента РФ утверждается «Перечень сведений, отнесенных к государственной тайне». В начале 1996 года утверждается «Положение о Межведомственной комиссии по защите государственной тайны» [5, с. 118].

Благодаря подписанию Окинавской хартии в то время были предприняты успешные попытки объединения России и других развитых стран для обеспечения безопасности мирового информационного сообщества, развития постиндустриального пространства, создания комфортных условий для обмена информацией между людьми и устранения проблем информационного неравенства [1]. Это стало важным толчком для развития общества XXI века.

Утверждение Доктрины информационной безопасности прояснило некоторые положения Концепции национальной безопасности Российской Федерации, появившейся в том же 2000 году 10 января [2]. Благодаря Доктрине был установлен официальный взгляд на национальные интересы в сфере информатизации, обеспечение безопасности этих интересов, в том числе создание методов противодействия угрозам и системы обеспечения информационной безопасности. Она объединила органы государственной власти в части согласования их деятельности в обеспечении защиты национальных интересов информационной сферы от внутренних и внешних угроз, а также положила начало практического участия Российской Федерации в реализации международных целей, прописанных в Окинавской хартии. Для этого был проанализирован прошлый опыт советского периода и периодов политических и социально-экономических преобразований. Создание информационных условий национальной безопасности, отмеченных в Доктрине, касается развития социальной, экономической и материальной составляющей информационного общества России и его институтов, а также знаменует информатизацию политической, социальной и духовной сфер общественной жизни, обеспечения международных стандартов поддержания прав личности.

В эти же годы находит свое развитие правовое регулирование информационной безопасности. Появляются такие законы, как «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене», «О связи», «О государственной тайне». С появлением первой и второй части изменяется Гражданский Кодекс Российской Федерации. Уголовный и Уголовно-процессуальный Кодекс Российской Федерации выходят в новых редакциях. Утверждаются законы о регулировании средств массовой информации и деятельности органов исполнительной власти по противодействию угрозам национальных интересов информационной без-

опасности [7, с. 68]. Все это способствует и развитию средств безопасности в Интернете, сетях связи и автоматизированных системах, использующихся в работе производств и предприятий.

Современное общество активно использует информационную среду не только для собственного развития, но и для преобразования социально-политической и экономической сфер жизни. Это связано с потребностью активной части общества реализовывать свои конституционные права на развитие экономической, интеллектуальной и, в первую очередь, информационной деятельности, путем информационной коммуникации не только внутри страны, но и за ее пределами. Так, по данным всемирной организации ЮНЕСКО были отмечены самые популярные виды связи: мобильная и Интернет. При этом в России уже к 2000 году насчитывалось порядка 2 млн. человек, зарегистрированных в Интернете. Из них активными пользователями были не менее 1,2 млн. человек [9, с. 43]. На начало 2023 года в РФ таких пользователей уже 127,6 млн. человек и их число продолжает активно расти.

Тем самым нужно понимать, что информационная сфера занимает значительное место в жизни нашего государства. Поэтому зависимость России от информационного общества дает важный толчок к обеспечению безопасности интересов этого общества и страны в целом.

Перечисление национальных интересов в сфере информации было утверждено и закреплено в Доктрине информационной безопасности Российской Федерации 2006 года. Эти интересы включают в себя следующее:

– соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

– информационное обеспечение государственной политики Российской Федерации;

– развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем как уже развернутых, так и создаваемых на территории России [2].

Все это необходимо для грамотного формирования российского информационного общества в XXI веке. Имеется ввиду такой подход к обществу, который поможет развивать людям свои возможности в информационной сфере, благодаря эффективному использованию интеллектуальных технологий. Если вернуться к Окинавской Хартии глобального информационного общества, то похожее можно увидеть в одной из ее задач. Здесь описано, что главы всех государств, подписавших документ, должны обеспечить людям беспрепятственный доступ к преимуществам глобального информационного общества [1]. Из этого следует, что Россия подготовилась к полномасштабному участию в обеспечении национальной безопасности страны, благодаря решению име-

ющихся проблем и тех, которые могут появиться в процессе реализации задач, требующих более длительного времени для их решения.

Что касается вышеуказанных национальных интересов, описанных в Доктрине информационной безопасности Российской Федерации, здесь необходимо, в первую очередь, обратить внимание на духовное возрождение многонациональности народа России, объединении общества страны и повышение эффективности информационной сферы для удовлетворения интересов общества. Конечно, реализация этого в современных условиях довольно непростая задача. Это связано с имеющимся до сих пор расколом на бедных и богатых, вследствие чего происходит неравное использование ресурсов информационных технологий. Создание равных условий для каждого члена общества возможно путем образования специализированных социальных институтов поддержки жителей, которым требуется повышение квалификации в вопросе информатизации.

26 июля 2006 года был утвержден Федеральный закон Российской Федерации № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4]. Это один из основополагающих нормативных документов, регулирующих правовые отношения во время поиска, передачи и распространения информации.

Еще одним наиболее важным документом для развития информационного общества России стала Стратегия развития информационного общества в Российской Федерации [3]. Этот документ впервые был утвержден в 2008 году и положил начало активному использованию коммуникационных технологий гражданами, бизнесом и органами государственной власти. Согласно положениям Стратегии целью развития и формирования информационного общества служило повышение качества жизни граждан, конкурентоспособности страны, совершенствование социально-политической, экономической, культурной и духовной ее части, улучшение государственного управления в сфере информационных технологий.

В 2017 году Президентом Российской Федерации была утверждена новая Стратегия развития информационного общества Российской Федерации на 2017-2030 годы [3]. Здесь уже цели направлены на защиту национальных интересов общества. Описаны меры по реализации внешней и внутренней политики России в части коммуникационных и информационных технологий для развития информационного общества, которое определяется здесь, как общество, непосредственно меняющее социальные, культурные и экономические сферы жизни граждан путем доступности и применения информации.

Еще одним важным изменением в новой редакции стала задача развития цифровой экономики в России. Цифровая экономика – это такая деятельность, где основным фактором производства становятся цифровые данные, обрабатываемые в большом количестве, а анализ их результатов позволяет в значительной мере увеличить эффективность любого рода производства, технологий, обработки, хранения, оборудования, продажи, доставки товаров и услуг. Для реализации развития этого направления вслед за новой Стратегией развития была утверждена национальная программа «Цифровая экономика Российской Федерации».

Можно с уверенностью сказать, что информационные технологии влияют на экономику Российской Федерации. Это определяется количеством активных пользователей в сетях Интернета, которые ежедневно используют их для приобретения коммерческих товаров и услуг, получения государственных услуг и совершения денежных пе-

реводов. Однако, несмотря на большое количество людей, использующих информационные технологии, частота их использования для эффективности развития в части экономики все еще мала. Все-таки цифровая экономика подразумевает использование более наукоемких технологий для ускорения процесса производства и обработки большого количества данных за короткий промежуток времени. А современная экономика в России строится на наработках зарубежных компаний, что может привести к нарушению информационной безопасности [8, с. 73].

Информационные ресурсы составляют основу духовного и научно-технического потенциала России. Поэтому их необходимо использовать рационально и сохранять, не нарушая при этом конституционные права граждан, обеспечив им свободный доступ к получению, передаче, поиску и распространению информации законными способами.

Так как современные достижения научно-технического прогресса, новейшие информационно-телекоммуникационные технологии могут быть использованы и уже используются в преступных целях, реализация положений Стратегии развития информационного общества на 2017-2030 годы невозможна без принятия адекватных мер по обеспечению информационной безопасности. И чем развитее будет информационное общество, тем больше сил и средств потребуется государству, чтобы обеспечить его безопасность. Ведущую роль в создаваемом механизме обеспечения национальной безопасности должно играть право со всеми присущими ему методами и средствами. Арсенал технологий воздействия на информационную сферу, систему социальных отношений государства, индивидуальное и массовое сознание общества в настоящее время разнообразен и характеризуется высокой степенью опасности. В этих условиях наиболее подвержены опасности национальные интересы РФ в информационной сфере. В то же время развитие правового регулирования в информационной сфере будет существенным образом обеспечивать информационную безопасность РФ, что, в свою очередь, будет способствовать обеспечению национальной безопасности РФ в целом.

Литература

1. Окинавская Хартия глобального информационного общества: Международный договор Хартия от 22.07.2000 // Дипломатический вестник. – 2000. – № 8.

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

3. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента РФ от 09.05. 2017 № 203 // Собрание законодательства Российской Федерации. – 2017. – № 20. – Ст. 2901.

4. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий: Международное соглашение от 28.09.2018 // Собрание законодательства Российской Федерации. – 2022. – № 33. – Ст. 5883.

5. Бабаш А.В. Информационная безопасность. История защиты информации в России. – Москва: Книжный дом «Университет» (КДУ), 2018. – 172 с.

6. Бондарев В.В. Введение в информационную безопасность автоматизированных систем. – Москва: Московский Государственный Технический Университет (МГТУ) имени Н.Э. Баумана, 2018. – 585 с.

7. Васильков А.В. Безопасность и управление доступом в информационных системах: Учебное пособие. – Москва: Форум, 2021. – 463 с.

8. Глинская Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие. – Москва: ИНФРА-М, 2020. – 118 с.

9. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. – Москва: Радио и связь, 2018. – 176 с.

10. Клейменов С.А. Информационная безопасность и защита информации: Учебное пособие для студентов высших учебных заведений. Гриф УМО МО РФ. – Москва: Академия (Academia), 2020. – 692 с.

11. Крылов Г.О. Базовые понятия информационной безопасности: Учебное пособие. – Москва: Русайнс, 2021. – 522 с.

12. Познышев С.В. Основные начала науки уголовного права. Общая часть уголовного права. – Москва, 1912. – С. 133.

13. Спасович В.Д. Учебник уголовного права. Часть Общая. – СПб., 1863. – 104 с.

14. Федоров А.В. Информационная безопасность. Политическая теория и дипломатическая практика: Монография. – Москва: МГИМО-Университет, 2019. – 653 с.

15. Ярочкин В. Безопасность информационных систем. – Москва: Ось-89, 2021. – 320 с.

References

1. Okinawan Charter of the Global Information Society: International Treaty Charter dated 07/22/2000 // Diplomatic Bulletin. – 2000. – No. 8.

2. On the approval of the Information Security Doctrine of the Russian Federation: Decree of the President of the Russian Federation dated 05.12.2016 No. 646 // Collection of Legislation of the Russian Federation. – 2016. – No. 50. – St. 7074.

3. On the approval of the Information Security Doctrine of the Russian Federation : Decree of the President of the Russian Federation dated 05.12.2016 No. 646 // Collection of Legislation of the Russian Federation. – 2016. – No. 50. – St. 7074.

4. Agreement on cooperation of the member States of the Commonwealth of Independent States in combating crimes in the field of information technology: International Agreement dated 09/28/2018 // Collection of legislation of the Russian Federation. – 2022. – No. 33. – Article 5883.

5. Babash A.V. Information security. The history of information protection in Russia. – Moscow: University Book House (KDU), 2018. – 172 p.

6. Bondarev V.V. Introduction to information security of automated systems. – Moscow: Bauman Moscow State Technical University (MSTU), 2018. – 585 p.

7. Vasilkov A.V. Security and access control in information systems. Textbook. – Moscow: Forum, 2021. – 463 p.

8. Glinskaya E.V. Information security of computer structures and systems. Textbook. – Moscow: INFRA-M, 2020. – 118 p.

9. Devyanin P.N. Security analysis of access control and information flows in computer systems. – Moscow: Radio and Communications, 2018. – 176 p.

10. Kleimenov S.A. Information security and information protection. A textbook for students of higher educational institutions. Vulture of the Ministry of Defense of the Russian Federation. – Moscow: Academia, 2020. – 692 p.

11. Krylov G.O. Basic concepts of information security. Textbook. – Moscow: Rusains, 2021. – 522 p.

12. Poznyshev S.V. The basic principles of the science of criminal law. The general part of criminal law. – Moscow, 1912. – P. 133.

13. Spasovich V.D. Textbook of criminal law. General Part. – St. Petersburg, 1863. – 104 p.

14. Fedorov A.V. Information security. Political theory and diplomatic practice: monograph. – Moscow: MGIMO University, 2019. – 653 p.

15. Yarochkin V. Security of information systems. – Moscow: Os-89, 2021. – 320 p.