IV. УГОЛОВНОЕ ПРАВО И ПРОЦЕСС

Информация для цитирования:
Ефремова М. А. Социальная обусловленность уголовно-правовой охраны информационной безопасности Российской Федерации // Вестник Пермского университета. Юридические науки. 2017. Вып. 36. С. 222–230. DOI: 10.17072/1995-4190-2017-36-222-230.
Efremova M. A. Sotsial'naya obuslovlennost' ugolovno-pravovoy okhrany informatsionnoy bezopasnosti Rossiyskoy Federatsii [Social Conditionality of Criminal Law Protection of Information Security in the Russian Federation]. *Vestnik Permskogo Universiteta. Juridicheskie Nauki* – Perm University Herald. Juridical Sciences. 2017. Issue 36. Pp. 222–230. (In Russ.). DOI: 10.17072/1995-4190-2017-36-222-230.

УДК 343.45
DOI: 10.17072/1995-4190-2017-36-222-230

СОЦИАЛЬНАЯ ОБУСЛОВЛЕННОСТЬ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

М. А. Ефремова

Кандидат юридических наук, доцент, профессор кафедры
основ организации и управления в органах прокуратуры
Казанский юридический институт (филиал)
Академии Генеральной прокуратуры Российской Федерации
420021, Россия, г. Казань, ул. Московская, 41
ResearcherID: E-6250-2016
ORCID: 0000-0001-6037-6921
Статьи в БД «Scopus» / «Web of Science»:
DOI: 10.14505/jarle.v7.1(15).11
e-mail: seamaid63@gmail.com

Введение: *одной из составляющих национальной безопасности Российской Федерации является информационная безопасность. В последнее время роль информационной составляющей национальной безопасности существенно возросла. Появились новые вызовы и угрозы информационной безопасности Российской Федерации, которые требуют реакции законодателя. Уголовное законодательство нуждается в модернизации с целью усиления его эффективности в части уголовно-правовой охраны информационной безопасности. Об этом свидетельствует совокупность факторов, которые обусловливают необходимость усиления уголовно-правовой охраны информационной безопасности.* ***Цель:*** *исследовать совокупность факторов, обусловливающих усиление уголовно-правовой охраны информационной безопасности.* ***Методы:*** *методологическую основу исследования составляет совокупность методов научного познания: общенаучные методы (материалистической диалектики), частнонаучные методы (системно-структурный, сравнительно-правовой и др.).* ***Результаты:*** *уголовно-правовая охрана информационной безопасности Российской Федерации в настоящее время не отвечает современным реалиям. Социально-экономический, исторический, политический, социально-правовой и криминологический факторы свидетельствуют о необходимости принятия законодательных мер.* ***Выводы:*** *нормы УК РФ, направленные на уголовно-правовую охрану информационной безопасности, нуждаются в совершенствовании.*

Ключевые слова: информация; информационная безопасность;
компьютерная информация; защита информации; уголовный закон

© Ефремова М. А., 2017

SOCIAL CONDITIONALITY OF CRIMINAL LAW PROTECTION OF INFORMATION SECURITY IN THE RUSSIAN FEDERATION

M. A. Efremova

Kazan Law Institution (branch) of the Academy
of the Prosecutor General's Office of the Russian Federation
41, Moskovskaya st., Kazan, 420021, Russia
ResearcherID: E-6250-2016
ORCID: 0000-0001-6037-6921
Articles in DB "Scopus" / "Web of Science":
DOI: 10.14505/jarle.v7.1(15).11
e-mail: seamaid63@gmail.com

Introduction: *information security is one of the components of the national security of the Russian Federation. Recently, the role of the information component of national security has increased significantly. There are new challenges and threats to the information security of the Russian Federation that require reaction of the legislator. Criminal legislation needs modernization to improve its efficiency in terms of criminal law protection of information security. This is evidenced by a combination of factors that determine the need to strengthen the criminal law protection of information security.* ***Purpose:*** *to study the factors that necessitate the strengthening of criminal law protection of information security.* ***Methods:*** *the methodological framework of the research is based on a set of scientific methods, including general scientific methods (materialist dialectic) and specific scientific ones (systemic-structural, comparative law and others).* ***Results:*** *at present, criminal law protection of information security of the Russian Federation does not meet the modern realities. Socio-economic, historical, political, socio-legal and criminological factors indicate the necessity of adopting legislative measures.* ***Conclusions:*** *regulations of the Criminal Code of the Russian Federation on criminal law protection of information security require improvement.*

Keywords: information; information security; computer information; information protection; criminal law

Введение

В новой редакции Стратегии национальной безопасности Российской Федерации[1] вопросы обеспечения информационной безопасности включены практически во все разделы, посвященные реализации стратегических национальных приоритетов. Это означает тесную взаимосвязь национальной безопасности и безопасности в информационной сфере. Здесь же находит проявление дуалистичность информационной безопасности. С одной стороны, она является частью национальной безопасности и в этом качестве выступает одним из элементов сложной многоуровневой системы различных видов безопасности, направленной на достижение состояния защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Обозначенные в Стратегии положения получили свое развитие и в новой редакции Доктрины информационной безопасности Российской Федерации[2]. В этом документе не только дана оценка современному состоянию информационной безопасности Российской Федерации, но и определен перечень угроз, а также совокупность средств, способных обеспечить должный уровень защиты информационной безопасности Российской Федерации. При этом правовые средства обеспечения информационной безопасности отнесены к приоритетному направлению деятельности.

Говоря о правовом инструментарии обеспечении информационной безопасности, следует отметить, что в наименьшей степени использован потенциал уголовно-правовых средств. Рассматривая информационную безопасность как объект уголовно-правовой охраны, следует понимать под таковой открытую динамичную си-

[1] *Стратегия* национальной безопасности Российской Федерации: утв. указом Президента Рос. Федерации от 31 дек. 2015 г. № 683. URL: http://kremlin.ru/acts/news/51129 (дата обращения: 20.03.2016).

[2] *Доктрина* информационной безопасности Российской Федерации: утв. указом Президента Рос. Федерации от 5 дек. 2016 г. № 646.

стему общественных отношений, обеспечивающих реализацию интересов личности, общества и государства в информационной сфере. Однако нормы, направленные на уголовно-правовую охрану информационной безопасности, помещены в различные разделы и главы УК РФ, что едва ли отвечает интенсивным темпам развития информационных технологий. Уголовное законодательство должно отражать изменения видов преступлений, посягающих на информационную безопасность. Поэтому необходимы переосмысление информационной безопасности как социальной ценности и принятие адекватных мер уголовно-правового реагирования за посягательства на нее. Основой эффективности правовых норм следует считать их социальную обусловленность. Несмотря на то, что нормы уголовного права, равно как и нормы всех других отраслей права, получают закрепление в отечественном законодательстве в результате сознательной человеческой деятельности, их истоки следует искать в закономерностях общественного развития. Непосредственным основанием уголовно-правовой охраны является социальная потребность в охране той или иной группы общественных отношений [11, с. 46–48]. Таким образом, природа уголовного закона, прежде всего, сводится к объективным законам общественного развития, когда появляется необходимость в охране общественных отношений, ставших особо значимыми, ценными для общества на соответствующем временном этапе.

Понятие социальной обусловленности является весьма широким, состоящим из множества объективных факторов, которые в совокупности и выступают индикаторами необходимости модификации уголовного закона. По нашему мнению, к факторам, обусловливающим необходимость выделения информационной безопасности как объекта уголовно-правовой охраны, следует отнести: социально-экономический, исторический, политический и социально-правовой.

Социально-экономические предпосылки уголовно-правовой охраны информационной безопасности

Основополагающей и ведущей является социально-экономическая обусловленность правовых норм. «Соответствие законов юридических законам экономического развития общества – важнейшая предпосылка их эффективности» [8, с. 101]. В этой связи представляется логичным в первую очередь рассмотреть подробнее указанный фактор.

Социально-экономические предпосылки уголовно-правовой охраны информационной безопасности вызваны, прежде всего, тем, что Российская Федерация входит в новую постиндустриальную стадию развития – так называемое «информационное общество». Становление информационного общества в России требует переосмысления иерархии охраняемых уголовным законом общественных отношений. Термин «информационное общество» практически одновременно был введен американским экономистом Ф. Машлупом, исследовавшим информационный сектор экономики на примере США, и профессором Токийского технологического института Ю. Хаяши в отчетах, представленных японскому правительству Агентством экономического планирования, Институтом разработки использования компьютеров, Советом по структуре промышленности. В этих отчетах информационное общество определялось как общество, в котором развитие компьютерных технологий сможет обеспечить его гражданам доступ к надежным источникам информации и высокий уровень автоматизации производства.

Концепцию постиндустриального информационного общества разработали западные социологи: Д. Белл, Дж. Гелбрейт, Дж. Мартин, И. Масуде, Ф. Полак, Э. Тоффлер. В России же исследованием концепции информационного общества занимались В. М. Глушков, Н. Н. Моисеев, А. И. Ракитов, А. В. Соколов, А. Д. Урсул и др.

Нельзя не отметить, что многие ведущие мировые державы уже вступили в стадию, именуемую информационным обществом, а на международном уровне был принят целый ряд правовых актов по вопросам развития информационного общества [13; 17]. Так, 22 июля 2000 г. лидерами стран «большой восьмерки» была подписана Окинавская хартия глобального информационного общества. Хартия явилась, прежде всего, призывом ко всем как в государственном, так и в частном секторах ликвидировать международный разрыв в области информации знаний. В качестве главенствующей задачи, стоящей перед государствами, Хартия провозгласила не только стимулирование и содействие переходу к информационному обществу, но также и реализации его полных экономических, социальных и культурных преимуществ[1]. В 2003 г. была принята Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии»[2], а в мае 2005 г. – Деклара-

[1] *Окинавская* хартия глобального информационного общества // Дипломат. вестник. 2000. № 8. С. 51–56.

[2] *Декларация* принципов «Построение информационного общества – глобальная задача в новом тысячелетии»: док. WSIS-03/GENEVA/DOC/4-R 12.12.2003. URL: http://www.

ция Комитета министров Совета Европы о правах человека и верховенстве права в информационном обществе[1].

Что касается Российской Федерации, то основополагающим документом в этой области стала Стратегия развития информационного общества[2]. В Стратегии учтены основные положения Окинавской хартии глобального информационного общества, Декларации принципов построения информационного общества и других международных документов, принятых на Всемирной встрече на высшем уровне по вопросам развития информационного общества.

Целью формирования и развития информационного общества в Российской Федерации, согласно положениям Стратегии, является повышение качества жизни граждан, обеспечение конкурентоспособности России, развитие экономической, социально-политической, культурной и духовной сфер жизни общества, а также совершенствование системы государственного управления на основе использования информационных технологий.

Информационное общество характеризуется возрастающей ролью информационной сферы, представляющей собой «совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом является совокупностью общественных отношений, связанных с информацией и информационной инфраструктурой как объектами интересов индивида, общества и государства [9, с. 56]. Очевидно, что феномен информации является основным элементом информационной сферы и, соответственно, всех информационных процессов, происходящих в обществе [5, с. 28].

Отличительными особенностями и характеристиками информационного общества ученые называют:

– развитие рынка информационно-телекоммуникационных технологий;

– зависимость экономики от уровня развития информационно-телекоммуникационных технологий в отдельно взятой стране;

– массовое использование компьютеров, имеющих доступ к информационно-телекоммуникационным сетям, и наличие навыков у населения по работе с такими компьютерами;

– возможность свободно искать, получать информацию из информационных ресурсов, а также и распространять и передавать через информационно-телекоммуникационные сети;

– увеличение требований к информационной безопасности для защиты интересов личности общества и государства в информационной сфере [3, с. 22; 6, с. 95–100].

Конечной эволюционной точкой развития информационного общества в отдельном государстве является интеграция в глобальное информационное общество. Отличительными чертами последнего выступают:

– формирование в результате социальной революции, носящей глобальный характер и имеющей своей основой интенсивное развитие и конвергенцию информационно-телекоммуникационных технологий;

– залогом благополучия как отдельного человека, так и отдельного государства является знание, которое было получено ввиду наличия свободного доступа к информации и умению работать с ней;

– процесс обмена информацией не имеет каких-либо границ;

– взаимопроникновение культур и в то же время появление новых возможностей для реализации [7, с. 161].

В 2013 году Россия заняла 40-е место в рейтинге стран по индексу развития ИКТ [14]. Для расчета Индекса используется 11 показателей, характеризующих проникновение фиксированной телефонной связи, мобильной сотовой связи и Интернета (в том числе широкополосного), доступ к компьютерам и интернету домохозяйств, уровень грамотности взрослого населения и вовлеченность в образование молодежи. Место России в рейтинге стран по этому Индексу входит в число контрольных показателей Стратегии развития информационного общества в Российской Федерации и государственной программы «Информационное общество (2011–2020 годы)»[3]. Контрольные показатели указаны в приложении к Стратегии, а их достижение должно свидетельствовать об интенсивности развития информационного общества в Российской Федерации. И Стратегия, и программа реализуются в несколько этапов. Выделение этапов

itu.int/dms_pub/itu-s/md/03/wsis/doc/s03-wsis-doc-0004!!pdf-r.pdf (дата обращения: 15.02.2016).

[1] *Декларация* Комитета министров о правах человека и верховенстве права в Информационном обществе: док. CM(2005)56 final 13.05.2005. URL: http://www.coe.int/ru/ (дата обращения: 15.02.2016).

[2] *Стратегия* развития информационного общества в Российской Федерации: утв. указом Президента Рос. Федерации от 7 февр. 2008 г. № Пр-212 // Рос. газета. 2008. 16 февр.

[3] *Об утверждении* государственной программы Российской Федерации «Информационное общество (2011–2020 годы)»: постановление Правительства Рос. Федерации от 15 апр. 2014 г. № 313 // Собр. законодательства Рос. Федерации. 2014. № 18, ч. II, ст. 2159.

обусловлено необходимостью подведения итогов выполнения Стратегии и уточнения задач развития информационного общества. При реализации инновационного сценария Программа не только решает задачи в сфере информационных технологий, но и становится инструментом решения задач модернизации в иных сферах (управление, образование, здравоохранение и др.), регионального развития и интеграции в мировое хозяйство, повышения качества человеческого капитала и стандартов жизни населения. А к 2020 году прогнозируется 10-кратный рост объема услуг связи (в 2,6 раза к 2015 г. относительно 2010 г. и в 2,7 раза за время реализации второго этапа Программы в 2015–2020 гг.) и более чем 2-кратный рост объема рынка информационных технологий. Однако уже в 2014 и 2015 гг. показатели России в рейтинге ухудшились, наша страна занимала 42-е и 45-е место.

В то же время в Российской Федерации уже создана достаточная база для становления и развития информационного общества. В самой Стратегии развития информационного общества в Российской Федерации отмечается, что увеличение добавленной стоимости в экономике достигается преимущественно за счет интеллектуальной деятельности, росту технологического уровня производства и масштабного внедрения новейших информационно-телекоммуникационных технологий. Хозяйственные системы постепенно интегрируются в экономику знаний, интеллектуальные факторы производства в которой играют роль локомотива.

Так как современные достижения научно-технического прогресса, новейшие информационно-телекоммуникационные технологии могут быть использованы и уже используются в преступных целях [12; 15; 16], залогом успешного становления информационного общества в России является обеспечение безопасности в информационной сфере. И чем развитее будет информационное общество, тем больше сил и средств потребуются государству, чтобы обеспечить его безопасность. Ведущую роль в создаваемом механизме обеспечения национальной безопасности должно играть право со всеми присущим ими ему методами и средствами.

Таким образом, социально-экономический фактор обусловленности уголовно-правовой охраны информационной безопасности связан с развитием в нашей стране нового типа общества, в котором во главе угла стоят информационно-коммуникационные технологии. Экономическое развитие государства также зависит от этих технологий – сырьевая экономика превращается в экономику информации и знаний. Духовные и социальные потребности у людей теперь ориентированы на быстрый поиск необходимой информации, своевременное и полное получение достоверной информации, возможность оперативного обмена ею.

Исторические предпосылки уголовно-правовой охраны информационной безопасности

Следующий фактор – исторической обусловленности уголовно-правовой охраны информационной безопасности предполагает эволюционное развитие законодательства в этом направлении. Как уже неоднократно отмечалось в данном исследовании, нормы, направленные на уголовно-правовую охрану информационной безопасности, содержатся в различных разделах и главах УК РФ. В 1996 году в УК РФ была включена гл. 28 «Преступления в сфере компьютерной информации», а в 2011 г. в гл. 28 УК РФ были внесены кардинальные изменения – все три ее статьи предстали в новой редакции. В научной литературе подчеркивалась необходимость совершенствования норм гл. 28 УК РФ, что и произошло спустя 15 лет после принятия самого УК. Интенсивность развития информационных технологий вызывает необходимость в изменении законодательства. Уголовное законодательство должно отражать изменения видов преступлений, посягающих на информационную безопасность. Поэтому следующим этапом должно стать переосмысление информационной безопасности как социальной ценности и принятие адекватных мер уголовно-правового реагирования за посягательства на нее.

Политические предпосылки уголовно-правовой охраны информационной безопасности

Политический фактор связан с задачами, стоящими перед Российской Федерацией, как во внутренней, так и внешней политике. В соответствии со ст. 4 ФЗ «О безопасности»[1], частью внутренней и внешней политики Российской Федерации является государственная политика в области обеспечения безопасности, которая представляет собой совокупность скоординированных и объединенных единым замыслом политических, организационных, социально-экономических, военных, правовых, информационных, специальных и иных мер. В последнее время появились новые вызовы и угрозы национальной безопасности России, которые нашли отражение в новой Стратегии национальной безопасности Российской Федерации, утвер-

[1] *О безопасности:* Федер. закон Рос. Федерации от 28 дек. 2010 г. № 390-ФЗ // Собр. законодательства Рос. Федерации. 2011. № 1, ст. 2.

жденной указом Президента Российской Федерации от 31 декабря 2015 г. № 683. В этом документе отмечается, что проведение Российской Федерацией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, которые оказывают на нашу страну политическое, экономическое, военное и информационное давление. В Стратегии подчеркивается, что все большее влияние на характер международной обстановки оказывает усиливающееся противоборство в глобальном информационном пространстве, обусловленное стремлением некоторых стран использовать информационные и коммуникационные технологии для достижения своих геополитических целей, в том числе путем манипулирования общественным сознанием и фальсификации истории. Появляются новые формы противоправной деятельности, в частности с использованием информационных, коммуникационных и высоких технологий. В числе угроз государственной и общественной безопасности, помимо прочих, в данном документе названа деятельность, связанная с использованием информационных и коммуникационных технологий для распространения и пропаганды идеологии фашизма, экстремизма, терроризма и сепаратизма, нанесения ущерба гражданскому миру, политической и социальной стабильности в обществе. Среди главных направлений обеспечения государственной и общественной безопасности в Стратегии говорится о совершенствовании правового регулирования предупреждения преступности, в том числе в информационной сфере, для чего совершенствуется система выявления и анализа угроз в информационной сфере, противодействия им. Иными словами, вопросы обеспечения информационной безопасности включены практически во все разделы, посвященные реализации стратегических национальных приоритетов, из чего можно сделать вывод о переоценке роли информационной безопасности в системе обеспечения национальной безопасности.

Социально-правовые предпосылки уголовно-правовой охраны информационной безопасности

Немаловажную роль играет и социально-правовой фактор. Как уже говорилось выше, борьба с преступностью в информационной сфере является одним из главных направлений обеспечения государственной и общественной безопасности, что, безусловно, связано с возросшей степенью общественной опасности преступных посягательств в информационной сфере. Информационная сфера, несмотря на ее значимость, является одной из самых незащищенных и поэтому уязвимых для различных форм противоправной деятельности. Рассредоточенные по всему УК РФ нормы, направленные на охрану информационной безопасности, не могут быть эффективным инструментом борьбы с преступностью в информационной сфере.

В настоящее время в нашей стране вновь наметилась тенденция к росту компьютерных преступлений, которые являются лишь частью преступлений против информационной безопасности. Об этом наглядно свидетельствуют и статистические данные. Так, в 2011 г. было зарегистрировано 2698 преступлений в сфере компьютерной информации, в 2012 г. – 2820, в 2013 г. – 2563, в 2014 г. – 1739, а в 2015 г. – 2382. После некоторого спада в 2015 г. вновь наблюдается рост преступности в сфере компьютерной информации. Вместе с тем, по оценкам одних специалистов, ущерб от такого рода преступлений в России в 2015 г. составил 1 млрд дол. Согласно же другим оценкам, этот ущерб составляет гораздо большую сумму. Преступления в сфере компьютерной информации характеризуются высокой степенью латентности, поэтому едва ли официальная статистика может отразить реальную картину.

У. В. Зинина обоснованно отмечает, что реальная статистика раскрываемости преступлений в сфере компьютерной информации в России искажена в результате не всегда правильного применения в следственной и судебной практике норм гл. 28 УК РФ, в том числе из-за расширительного толкования элементов, содержащихся в ней составов преступлений и фактического непонимания технических реалий [2, с. 13]. Поэтому официальные статистические данные, отражающие снижение преступности в сфере компьютерной информации, позволяют говорить о незначительной эффективности уголовно-правовых норм гл. 28 УК РФ, о высокой степени латентности данной группы преступлений и о необходимости принятия кардинальных мер.

Результаты

Прежде чем подвести итог, следует согласиться с Н. Ф. Кузнецовой и Г. А. Злобиным в том, что между социальной необходимостью и ее выражением в уголовном законе стоит исторически сформировавшееся общественно сознание данной эпохи, определяющее характер, формы и степень точности правовых отражений. Нормы права, в отличие от объективных законов природы, могут быть «хорошими» и «плохими», т. е. адекватно отражать общественную потребность или недостаточно соот-

ветствовать этой потребности, достигать или не достигать поставленных законодателем целей [4, с. 76]. Нормы УК РФ, направленные на уголовно-правовую охрану информационной безопасности, едва ли адекватно отражают общественную потребность в ее уголовно-правовой охране. Став новой ценностью, основой жизни движущим фактором развития экономики и производства, информация требует сосредоточения сил государства на создании условий для обеспечения ее безопасности. Сложившиеся социальные реалии обусловливают необходимость признания информационной безопасности как самостоятельного объекта уголовно-правовой охраны.

Недооценка значимости уголовно-правовых средств в механизме правового обеспечения информационной безопасности ставит под угрозу интересы личности, общества и государства в информационной сфере. А. А. Тер-Акопов подчеркивает, что сформировавшиеся информационные угрозы требуют более активной научной проработки. При этом особая роль принадлежит в этом вопросе уголовному праву, которое должно обобщить общественно опасные проявления посягательств на информационную безопасность человека, общества и государства [10, с. 165].

К наиболее актуальным угрозам информационной безопасности на современном относят:

– разработку, создание и использование средств воздействия и нанесения ущерба информационным ресурсам и телекоммуникационным системам государства;

– целенаправленное информационное воздействие на критически важные структуры;

– информационное воздействие, осуществляемое для подрыва политической, экономической и социальной системы государств, психологической обработки населения с целью дестабилизации общества;

– несанкционированное вмешательство в информационно-телекоммуникационные системы и информационные ресурсы, а также их неправомерное использование;

– деятельность международных террористических, экстремистских и преступных сообществ, организаций, групп и отдельных правонарушителей, представляющая угрозы информационным ресурсам и критически важным структурам государства;

– использование информационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационной сфере;

– трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальному законодательству государств [7, с. 242–249].

В Доктрине информационной безопасности РФ по общей направленности выделены следующие виды угроз информационной безопасности нашей страны:

– угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

– угрозы информационному обеспечению государственной политики Российской Федерации;

– угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

– угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Приведенные угрозы отражают негативные последствия информатизации, которые являются отнюдь не мифическими, а реальными. Прогнозируется и появление новых угроз, в связи с чем необходима основанная на едином критерии «упреждающая институционализация» [1] уголовно-правовых норм, направленных на уголовно-правовую охрану информационной безопасности.

Выводы

Таким образом, социальная обусловленность уголовно-правовой охраны информационной безопасности определяется совокупностью социально-экономических, исторических, политических и социально-правовых факторов. Указанные факторы выступают в качестве предпосылок криминализации деяний, посягающих на информационную безопасность. Специфичность названных факторов выражается в том, что все они связаны с процессом становления и развития информационного общества в Российской Федерации и свидетельствуют о необходимости расширении перечня запрещенных законом посягательств в информационной сфере.

Библиографический список

1. *Жук М. С.* Пути совершенствования системы институтов российского уголовного права // Lex Russica. 2015. № 4. С. 46–59.

2. *Зинина У. В.* Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дис. ... канд. юрид. наук. М., 2007. 33 с.
3. *Копылов В. А.* Информационное право. М.: Юристъ, 2004. 510 с.
4. *Кузнецова Н. Ф., Злобин Г. А.* Социальная обусловленность уголовного закона и научное обеспечение нормотворчества // Советское государство и право. 1976. № 8. С. 76–83.
5. *Куняев Н. Н.* Правовое обеспечение национальных интересов Российской Федерации в информационной сфере: дис. … д-ра юрид. наук. М., 2010. 420 с.
6. *Лопатин В. Н.* Информационная безопасность России: дис. ... д-ра юрид. наук. СПб., 2000. 433 с.
7. *Полякова Т. А.* Правовое обеспечение информационной безопасности при построении информационного общества в России: дис. … д-ра юрид. наук. М., 2008. 438 с.
8. *Реджепов А.* Социальная обусловленность уголовно-правовых норм как фактор повышения их эффективности // Тез. докл. на теор. конф. аспирантов Ин-та государства и права АН СССР и юрид. фак. МГУ им. М. В. Ломоносова. М.: Изд-во ИГиП АН СССР, 1981. С. 101–102.
9. *Стрельцов А. А.* Теоретические и методологические основы правового обеспечения информационной безопасности России: дис. … д-ра юрид. наук. М., 2004. 371 с.
10. *Тер-Акопов А. А.* Безопасность человека. Социальные и правовые основы. М., 2005. 272 с.
11. *Филимонов В. Д.* Норма уголовного права. СПб.: Изд-во Р. Асланова «Юридический центр Пресс», 2004. 198 с.
12. *Buchan R., Tsagourias N.* Cyber War and International Law // Journal of Conflict & Security Law. 2012. Vol. 17(2). P. 183–186.
13. *Maillard de J., Roche S.* Crime and justice in France; Trendsm Policies and Political Debate // European Journal of Criminology. 2004. January. Vol. 1. P. 111–151.
14. *Measuring* the Information Society. URL: http://d-russia.ru/wp-content/uploads/2013/11/MIS2013.pdf (дата обращения: 12.01.2016).
15. *Minott N.* The Economic Espionage Act: Is the Law All Bark and no Bite? // Information & Communications Technology Law. 2011. October. Vol. 20. P. 201–224.
16. *Mitrakas A.* Information security and law in Europe: Risks checked? // Information & Communications Technology Law. 2006. March. Vol. 15. P. 33–53.
17. *Ryder N., Reid A. S.* E-Crime // Information & Communications Technology Law. 2012. October. Vol. 21. P. 203–206.

References

1. *Zhuk M. S. Puti sovershenstvovaniya sistemy institutov rossiyskogo ugolovnogo prava* [Ways for the Improvement of the System of Institutions of the Russian Criminal Law]. *LEX RUSSICA*. 2015. Issue 4. Pp. 46–59. (In Russ.).
2. *Zinina U. V. Prestupleniya v sfere komp'yuternoy informatsii v rossiyskom i zarubezhnom ugolovnom prave: avtoref. dis. ... kand. yurid. nauk* [Crimes in the Sphere of Computer Information in Russian and Foreign Criminal Law: Synopsis of Cand. jurid. sci. diss]. Moscow, 2007. 33 p. (In Russ.).
3. *Kopylov V. A. Informatsionnoe pravo* [Information Law]. Moscow, 2004. 510 p. (In Russ.).
4. *Kuznetsova N. F., Zlobin G. A. Sotsial'naya obuslovlennost' ugolovnogo zakona i nauchnoe obespechenie normotvorchestva.* [The Social Conditionality of the Criminal Law and Scientific Support for Rule-Making]. *Sovetskoe gosudarstvo i pravo* – Soviet State and Law. 1976. Issue 8. Pp. 76–83. (In Russ.).
5. *Kunyaev N. N. Pravovoe obespechenie natsional'nykh interesov Rossiyskoy Federatsii v informatsionnoy sfere: dis. ... d-ra yurid. nauk* [The Legal Support for the National Interests of the Russian Federation in the Information Sphere: Dr. jurid. sci. diss]. Moscow, 2010. 420 p. (In Russ.).
6. *Lopatin V. N. Informatsionnaya bezopasnost' Rossii: dis. d-ra ... yurid. nauk* [Information Security of Russia: Dr. jurid. sci. diss]. St. Petersburg, 2000. 433 p. (In Russ.).
7. *Polyakova T. A. Pravovoe obespechenie informatsionnoy bezopasnosti pri postroenii informatsionnogo obshhestva v Rossii: dis. ... d-ra. yurid. nauk* [The Legal Support for Information Security When Developing Information Society in Russia: Dr. jurid. sci. diss]. Moscow, 2008. 438 p. (In Russ.).
8. *Redzhepov A. Sotsial'naya obuslovlennost' ugolovno-pravovykh norm kak faktor povysheniya ikh effektivnosti* [The Social Conditionality of Criminal Law Norms as a Factor in Increasing Their Effectiveness]. *Tezisy dokladov na teoreticheskoy konferentsii aspirantov Instituta gosudarstva i prava AN SSSR i yuridicheskogo fakul'teta MGU* – Abstracts of the Theoretical Conference of Post-Graduate Students of the Institute of State and Law of the USSR Academy of Sciences and the Faculty of Law of the Lomonosov Moscow State University. Moscow, 1981. Pp. 101–102. (In Russ.).

9. *Strel'tsov A. A. Teoreticheskie i metodologicheskie osnovy pravovogo obespecheniya informatsionnoy bezopasnosti Rossii: dis. ... d-ra yurid. nauk* [Theoretical and Methodological Basiss of the Legal Support for Information Security of Russia: Dr. jurid. sci. diss]. Moscow, 2004. 371 p. (In Russ.).
10. *Ter-Akopov A. A. Bezopasnost' cheloveka. Sotsial'nye i pravovye osnovy* [Human Security. Social and Legal Foundations]. Moscow, 2005. 272 p. (In Russ.).
11. *Filimonov V. D. Norma ugolovnogo prava* [The Rule of Criminal Law]. St. Petersburg, 2004. 198 p. (In Russ.).
12. *Buchan R., Tsagourias N.* Cyber War and International Law. *Journal of Conflict & Security Law*. 2012. Vol. 17(2). Pp. 183–186. (In Eng.).
13. *Maillard de J., Roche S.* Crime and justice in France; Trendsm Policies and Political Debate. *European Journal of Criminology.* 2004. January. Vol. 1. Pp. 111–151. (In Eng.).
14. *Measuring* the Information Society. Available at: http://d-russia.ru/wp-content/uploads/2013/11/MIS2013.pdf (accessed 12.01.2016). (In Eng.).
15. *Minott N.* The Economic Espionage Act: Is the Law All Bark and no Bite? *Information & Communications Technology Law.* 2011. October. Vol. 20. Pp. 201–224. (In Eng.).
16. *Mitrakas A.* Information security and law in Europe: Risks checked? *Information & Communications Technology Law.* 2006. March. Vol. 15. Pp. 33–53. (In Eng.).
17. *Ryder N., Reid A. S.* E-Crime. *Information & Communications Technology Law.* 2012. October. Vol. 21. Pp. 203–206. (In Eng.).