ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

К вопросу об информационной безопасности личности

Челенков Дмитрий Николаевич, студент магистратуры
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации (г. Москва)

В статье исследуются определение и содержание понятия «информационная безопасность личности». С позиций общественно-политических отношений и государственного управления рассматриваются вопросы нормативного правового и организационного обеспечения информационной безопасности личности в современной России.

Ключевые слова: *информационная безопасность, информационная безопасность личности, государственное регулирование.*

Эффективное функционирование государственных органов, реализация ими государственной политики предполагает, что это способствует развитию личности, общества, государства и бизнеса. При этом общественные отношения претерпевают постоянные изменения в процессе жизнедеятельности социума. В современном мире значительная часть жизни любого человека проходит в информационном пространстве. И вследствие стремительного развития информационных технологий в базах данных различных информационных ресурсов, как правило, подключенных к сети интернет, накапливается все больший массив информации, связанный с конкретным человеком. Очевидно, что должна обеспечиваться конфиденциальность определенного объема этой информации, должна быть обеспечена реализация законных прав граждан на передачу и получение информации. Кроме того, помимо угрозы разглашения личной информации, граждане подвергаются угрозам информационно-психологического воздействия или целенаправленным атакам с использованием информационных технологий. Результатом такого воздействия является ущерб, причиненный человеку (гражданину, личности). Это может быть финансовый, психологический ущерб, а с учетом развивающейся технологии интернета вещей (Internet of Things - IoT) и перспективных технологий интернета людей (Internet of Peaple - IoP) – и физический ущерб. В результате все более актуальным становится вопрос защиты граждан от информации и информационных технологий. Такова реальность продолжающейся информационной эры. В ближайшем будущем тенденции всеобщей «цифровизации» и «компьютеризации» будут только усиливаться. Исследования в области искусственного интеллекта являются одним из приоритетных направлений для всех ведущих в сфере науки стран, проводится подготовка к повсеместному внедрению «цифровых» паспортов, способных завершить окончательное формирование «цифровой» личности, все большее распространение приобретают «цифровые» валюты и т.д. Современная пандемия коронавирусной инфекции способствует стремительному развитию дистанционных технологий в области образования, переходу большого числа граждан на формат «удаленной» работы. Внедрение и использование каждой новой технологии влечет за собой и появление новых видов угроз.

Рассмотренные выше аспекты позволяют сделать вывод о важности выполнения следующих условий в интересах обеспечения информационной безопасности граждан: обеспечение конфиденциальности персональной информации граждан; их защита от влияния негативной или нежелательной информации; обеспечение защиты граждан от воздействий на них или принадлежащую им собственность информационных технологий. При этом не должны нарушаться законные права и свободы личности. Обеспечение выполнения указанных условий является одной из задач государственной политики.

В целом, основополагающими документами государственной политики России в области информационной безопасности являются Стратегия национальной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 31.12.2015 № 683, Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации от 05.12.2016 № 646. В определении основных терминов указанных документов присутствует сочетание понятий «личность», «общество», «государство». Так, Доктрина информационной безопасности Российской Федерации дает общее определение информационной безопасности, где одним из объектов защиты, наряду с обществом и государством, указана личность.

Вместе с тем, целесообразно более полное рассмотрение специфической области информационной безопасности личности, ввиду важности и сложности этого объекта. Сложность исследования объекта «личность» состоит в том, что, помимо объективных свойств, таких, как права и свободы, он обладает и субъективным свойством – сознание. Для формирования и реализации государственной политики в области информационной безопасности личности целесообразно уточнить сам объект государственной политики.

Анализ научных исследований и статей, касающихся вопроса определения информационной безопасности личности, позволяет получить представление о заинтересованности экспертов в сфере права и информационной безопасности в законодательном закреплении рассматриваемого понятия. К примеру, А.С. Жаров предлагает следующее определение: «информационная безопасность личности - это совокупность общественных отношений, складывающихся в процессе защиты ее конституционных прав и свобод от угроз в информационной сфере» [1].

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

В свою очередь, С.В. Нуянзин и О.С. Нуянзин учитывают сознание личности: «информационная безопасность личности - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию человека» [2]. С.В. Баринов предлагает обозначить в составе информационной безопасности личности четыре составляющие: информационно-техническую, информационно-идеологическую, информационно-психологическую и информационно-правовую безопасность личности [3].

Автору данной статьи представляется целесообразным при формулировании определения учесть объективные и субъективные свойства личности и не забывать о необходимости обеспечения не только защиты информации и защиты от информации, но и необходимости защиты информационной инфраструктуры, используемой личностью. При формулировании понятия информационной безопасности личности предлагается учесть следующие аспекты: защищенность личности от внутренних и внешних угроз, права и свободы личности, аспекты безопасности информации (конфиденциальность, целостность, доступность), защищенность информационной инфраструктуры. Целесообразно в качестве исходного определения использовать более широкое понятие информационной безопасности Российской Федерации, указанное в Доктрине информационной безопасности Российской Федерации. В такой трактовке информационная безопасность личности может пониматься как состояние защищенности личности и используемой ею информационной инфраструктуры от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, поддержание личной информации в целостности и сохранности, предотвращение несанкционированного доступа к ней, а также находятся в допустимых пределах риски, связанные с причинением информацией вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию личности. Подобное определение раскрывает основные направления, в соответствии с которыми целесообразно обеспечивать информационную безопасность личности.

Правовое закрепление определения информационной безопасности личности должно стать отправной точкой, от которой может в дальнейшем происходить формирование государственной политики в области информационной безопасности граждан. В частности, это должно повлечь за собой корректировку ряда задач государственных органов Российской Федерации, выполняющих регуляторную функцию в сфере информационной безопасности.

В настоящее время четко не определено, какой государственный орган и каким образом реализует функции государственного регулирования в области обеспечения информационной безопасности личности. При этом в России существуют несколько основных регуляторов в сфере информационной безопасности: Федеральная служба безопасности Российской Федерации (ФСБ РФ); Федеральная служба по техническому и экспортному контролю (ФСТЭК); Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифра); Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор); Центральный Банк Российской Федерации (ЦБ РФ) и другие.

Рассмотрим основные направления информационной безопасности, в рамках которых осуществляют свою деятельность перечисленные регуляторные органы Российской Федерации.

Полномочия ФСБ РФ в обеспечении информационной безопасности касаются, в основном, использования инженерно-технических и криптографических средств, сетей связи, связанных с передачей шифрованной информации, в Российской Федерации и ее учреждениях, находящихся за пределами России[4].

ФСТЭК отвечает за реализацию государственной политики по вопросам обеспечения безопасности критической информационной инфраструктуры и противодействия иностранным техническим разведкам [5].

Минцифра обеспечивает формирование и реализацию государственной политики и нормативно-правового регулирования в сфере информационных технологий, электросвязи и почтовой связи, массовых коммуникаций и средств массовой информации, обработки персональных данных, а также по выработке и реализации государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и (или) развитию [6].

Роскомнадзор выполняет функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных [7].

ЦБ РФ обладает полномочиями в области информационной безопасности, касающейся в основном кредитно-денежной системы.

Анализ полномочий указанных учреждений позволяет сделать вывод об отсутствии возложенных на какой-либо из государственных регуляторов функций, связанных с выработкой и реализацией государственной политики в области информационной безопасности личности, то есть о ведущей роли в этой сфере. Функции, выполняемые перечисленными государственными органами, направлены в основном на решение ведомственных задач в интересах государства. Это приводит к ряду негативных последствий: отсутствие эффективных мер по защите интересов граждан в информационном пространстве, отсутствие координации между государственными органами в случае масштабных атак в информационном пространстве, недостаточно быстрое реагирование на появляющиеся новые информационные угрозы и прочее. При этом очевидно, что часть задач, которые фактически выполняются в целях обеспечения информационной безопасности личности, в перечне функций у регуляторов присутствует. Например, вопросы, связанные с защитой персональных данных или защиты детей от вредной информации. В целом, деятельность государственных органов, в той или

иной степени отвечающих за обеспечение информационной безопасности, зачастую носит разрозненный характер.

Кроме того, в перечне сил обеспечения информационной безопасности Российской Федерации в соответствии с Доктриной информационной безопасности Российской Федерации указаны ряд государственных органов, призванных в первую очередь реагировать на большое количество существующих и появляющихся угроз информационной безопасности личности уже по факту их осуществления. Так, органы прокуратуры, МВД, судебные органы расследуют и выносят вердикты по осуществившимся правонарушениям в информационной сфере. Применение же превентивных мер в целях противодействия подобным угрозам в большей степени является личным делом каждого гражданина. Появляющиеся периодически в средствах массовой информации рекомендации специалистов в области информационной безопасности по способам противодействия и защиты от различного рода информационных угроз являются, без сомнения, ценными, но появление таких публикаций не носит системного характера, а количество граждан, ознакомившихся с подобными рекомендациями, ограничено числом читателей конкретного средства массовой информации.

Следует отметить, что необходимость выделения вопросов обеспечения информационной безопасности личности в отдельное направление государственной политики продиктовано не только стремительным развитием информационных технологий и сопутствующих им угроз, но и основополагающим законом Российской Федерации. В статье 71 Конституции Российской Федерации устанавливается, что в ведении Российской Федерации находится, в том числе, «обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных» [8]. Кроме того, согласно Стратегии национальной безопасности Российской Федерации: «интересы личности заключаются в реальном обеспечении своих конституционных прав и свобод, личной безопасности, повышении качества и уровня жизни, возможности физического, интеллектуального и духовного развития. Совокупность интересов личности, общества и государства составляют национальные интересы Российской Федерации» [9]. Таким образом, очевидна важность интересов личности для государственной политики в области национальной безопасности, в целом, и в области информационной безопасности, в частности.

Учитывая, что Конституцией Российской Федерации высшей ценностью признается человек, его права и свободы, а их защита является обязанностью государства, представляется целесообразным выделить в отдельное направление государственной политики сферу обеспечения информационной безопасности личности.

Опыт ведущих в вопросах обеспечения информационной безопасности стран показывает целесообразность создания и функционирования единого государственного органа в указанной сфере. Так в Сингапуре с 2015 года функционирует Национальное Агентство Кибербезопасности (Cyber Security Agency of Singapore - CSA), координирующее усилия государства в области информационной безопасности. Отношение официальных властей Сингапура к обеспечению информационной безопасности граждан показывает сравнение помощника начальника CSA Гаурава Киртхи информационной безопасности с общественным благом. По его словам, «правительство Сингапура будет намерено обеспечить гражданам и компаниям безопасную информационную среду точно так же, как обеспечивает их другими общественными благами, такими как водопровод и канализация» [10].

Представляется целесообразным определить единый государственный орган в Российской Федерации, координирующий деятельность остальных государственных органов в вопросах обеспечения информационной безопасности. Одним из направлений деятельности создаваемого государственного органа должно стать формирование государственной политики в области обеспечения информационной безопасности граждан. Кроме того, уполномоченный государственный орган также будет обеспечивать координацию деятельности всех заинтересованных органов, к которым, учитывая возможности государственно-частного партнерства, следует отнести и негосударственные организации, способные оказать поддержку в вопросах обеспечения информационной безопасности личности. Функции, которые, предположительно, мог бы выполнять указанный государственный орган в отношении информационной безопасности граждан, заключаются в следующем:

1. Разработка нормативно-правовых актов в области информационной безопасности личности в Российской Федерации.
2. Осуществление государственного регулирования и контроля в области информационной безопасности личности в Российской Федерации.
3. Осуществление мониторинга и анализа угроз информационной безопасности личности в Российской Федерации.
4. Осуществление взаимодействия с государственными и частными, в том числе международными, центрами кибербезопасности, осуществляющими реагирование на компьютерные инциденты, в целях сбора и анализа информации об угрозах.
5. Информирование граждан об угрозах информационной безопасности личности и методах противодействия им.
6. Организация обучения граждан правилам информационной безопасности личности.
7. Предоставление доступа гражданам Российской Федерации к инструментам обеспечения информационной безопасности личности.

Для выполнения вышеперечисленных функций уже существует определенный организационный и технический задел. Так, в рамках федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика» предусмотрено создание специализированного ресурса, предназначенного для взаимодействия с уполномоченными органами для оперативной передачи данных о противоправных действиях в области информацион-

www.esa-conference.ru

ных технологий (телефонное мошенничество, фишинговые схемы и т.д.). Планируется разработка модели угроз информационной безопасности для персональных устройств сбора биометрических данных (холтер, браслеты, часы, фитнес-трекеры и пр.) и дорожной карты по обеспечению информационной безопасности при использовании гражданами указанного класса технических средств в Российской Федерации. Активно используются подходы, связанные с информационной безопасностью в производственной сфере [11]. Также нормативно обеспечена предустановка отечественных антивирусных средств на все ввозимые и создаваемые на территории России персональные компьютеры [12].

Эти и ряд других мероприятий федерального проекта «Информационная безопасность» могут в дальнейшем послужить основой для реализации функций, стоящих перед государственным органом, осуществляющим регулирование в области информационной безопасности личности.

Отметим, что в настоящее время имеется высокая вероятность возникновения кризисных явлений в любой из сфер жизнедеятельности [13], что, несомненно, может привести к возникновению угроз безопасности личности. Особенно ярко это проявилось в связи с продолжающейся пандемией COVID-19, которая с самого начала сопровождается не менее опасной инфодемией. В этих условиях значительно возрастает роль антикризисного управления, предполагающего прогнозирование угроз, в том числе информационных угроз личности, их причин и симптомов, разработку мер мероприятий по недопущению, нейтрализации, снижению негативных последствий, использованию кризисных тенденций в интересах развития личности, общества, государства, бизнеса [14].

В целом, представленные в статье предложения являются одним из шагов к появлению Концепции развития сферы обеспечения информационной безопасности личности в Российской Федерации. При этом важно инициировать обсуждение терминологии информационной безопасности личности и способов регулирования данной сферы в Российской Федерации. Разработка, принятие и реализация такой Концепции позволит совершенствовать государственную политику в области информационной безопасности личности, предоставить гражданам Российской Федерации инструменты для обеспечения собственной информационной безопасности и вывести на более высокий уровень информационную грамотность граждан, что, в конечном итоге, положительно скажется на уровне социально-экономического развития и состоянии национальной безопасности Российской Федерации.

Литература:

1. А.С. Жаров. Конституционно-правовое регулирование информационной безопасности личности в Российской Федерации. Диссертация. 2006 год/ / Библиотека диссертаций. [Электронный ресурс]. URL: https://www.dissercat.com/chasto-zadavaemye-voprosy-pri-rabote-s-nashei-nauchnoi-bibliotekoi (дата обращения:03.01.2021).
2. Нуянзин С.В., Нуянзин О.С. Информационная безопасность личности и некоторые организационно-правовые меры по ее обеспечению / / Юридическая наука и правоохранительная практика. 2018. №2 (44). URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-lichnosti-i-nekotorye-organizatsionno-pravovye-mery-po-ee-obespecheniyu (дата обращения: 05.01.2021).
3. Баринов Сергей Владимирович. О правовом определении понятия «Информационная безопасность личности» / / Актуальные проблемы российского права. 2016. №4 (65). URL: https://cyberleninka.ru/article/n/o-pravovom-opredelenii-ponyatiya-informatsionnaya-bezopasnost-lichnosti (дата обращения: 05.01.2021).
4. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» / / СПС «Консультант Плюс» [Электронный ресурс] URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=367302&dst=100081%2C0#0542762274 0891451 (дата обращения: 05.01.2021).
5. Указ Президента РФ от 16.08.2004 № 1085 (ред. от 31.08.2020) «Вопросы Федеральной службы по техническому и экспортному контролю» / / СПС «Консультант Плюс» [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_14031/9b13a25cec35f1d26a1331611204f68c696b5c53 (дата обращения: 05.01.2021).
6. Постановление Правительства РФ от 02.06.2008 № 418 (ред. от 06.02.2020) «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации» / / СПС «Консультант Плюс» [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_77387 (дата обращения: 05.01.2020).
7. Постановление Правительства РФ от 16.03.2009 № 228 (ред. от 05.12.2019) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» / / СПС «Консультант Плюс» [Электронный ресурс] URL: //http://www.consultant.ru/cons/cgi/online.cgi?from=307806 (дата обращения: 05.01.2021).
8. Конституция РФ [Электронный ресурс] / / Государственная Дума Федерального Собрания Российской Федерации: [сайт]. [2021]. URL: http://duma.gov.ru/news/48953 (дата обращения: 4.01.2021 г.).
9. Указ Президента Российской Федерации от 31 декабря 2015 года № 683 «О Стратегии национальной безопасности Российской Федерации»/ / СПС «Консультант Плюс» [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_191669/ (дата обращения: 05.01.2021 г.).

www.esa-conference.ru

10. Власти Сингапура предложили относиться к ИБ как общественному благу [Электронный ресурс] / / SecurityLab.ru [сайт]. [01.10.2020]. URL: https://www.securitylab.ru/news/512644.php (дата обращения: 05.01.2021 г.).

11. Родионов М.А. Методологические аспекты информационного аудита в менеджменте предприятия. // Научный вестник МГТА ГА, № 156, М., 2010, С.68-74.

12. Паспорт федерального проекта Информационная безопасность [Электронный ресурс] / / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [сайт]. [2021]. URL: https://digital.ac.gov.ru/poleznaya-informaciya/material poleznaya-informaciya/material/Паспорт-федерального-проекта-Информационная-безопасность.pdf (дата обращения: 05.01.2021 г.).

13. Родионов М.А. Антикризисное управление. Часть 2. Практика антикризисного управления. М., МГТУ, 2014.

14. Артамонов Б.В., Родионов М.А. Концепция антикризисного менеджмента. // Научный вестник МГТУ ГА, № 131, М., 2008. С. 108-112.