DOI **10.37882/2223–2974.2023.03.06**

ПРОБЛЕМЫ РАЗВИТИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

PROBLEMS OF DEVELOPMENT OF THE INFORMATION SECURITY SYSTEM OF THE RUSSIAN FEDERATION

Ya. Vasileva
E. Kalinyuk

Summary. In this article, the concept of information security is considered from a scientific and legal point of view. The analysis of various problems of information security, such as: information leakage, cyberwar and cyberterrorism, and also presents ways to solve them both at the state and at the global level. The Institute of Information Security in Russia is represented at three levels: legislative, organizational, software and technical. Organizational information security is presented as a set of various measures aimed at protecting information from unauthorized access, planning and using material, financial and other resources, as well as managing them, in order to counter threats to information security. As part of solving problems in the field of information security, it is proposed first of all to improve regulatory and technical regulation, increase the level of legal culture and computer literacy of citizens, create secure information technologies, and ensure the technological independence of the state.

Keywords: information security, threats to information security, problems of information security.

Васильева Яна Валерьевна
Кандидат юридических наук, Северо-Западный институт (филиал) Университетf имени О.Е. Кутафина (МГЮА)
yana.vasileva@list.ru
Калинюк Екатерина Васильевна
Северо-Западный институт (филиал) Университета имени О.Е. Кутафина (МГЮА)
yekaterina.kalinyuk@yandex.ru

Аннотация. В данной статье с научной и правовой точек зрения рассматривается понятие информационной безопасности. Проводится анализ различных проблем информационной безопасности, таких как: утечка информации, кибервойна и кибертерроризм, а также представляются пути их решения как на государственном, так и на мировом уровне. Институт обеспечения информационной безопасности в России представляется в трех уровнях: законодательном, организационном, программно-техническом. Организационное обеспечение информационной безопасности представлено как совокупность различных мероприятий, направленных на защиту информации от несанкционированного доступа, планированию и использованию материальных, финансовых и иных ресурсов, а также управление ими, в целях противодействия угрозам информационной безопасности. В рамках решения проблем в сфере информационной безопасности предлагается в первую очередь совершенствовать нормативно-правовое и техническое регулирование, повышать уровень правовой культуры и компьютерной грамотности граждан, создавать безопасные информационные технологии, укреплять технологическую независимость государства.

Ключевые слова: информационная безопасность, угрозы информационной безопасности, проблемы информационной безопасности.

Актуальность темы исследования обусловлена тем, что в 21 веке получили стремительное распространение и развитие различные информационные технологии. Происходит постоянное увеличения объёма информации, которая фиксируется на электронных носителях, а также возрастает количество различных информационных систем. Внедрение информационных технологий обуславливает актуальность изучения проблем информационной безопасности: угрозы и проблемы, субъекты и законодательство в сфере обеспечения информационной безопасности, средства и меры ее защиты. В современных условиях информационная безопасность является одним из важнейших видов национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на законодательном, организационном и программно-техническом уровнях. Это необходимо для защиты информации от преступных и иных противоправных посягательств, соответственно, необходимо совершенствовать нормативно- правовую базу,

укреплять систему органов власти, обеспечивающих информационную безопасность, а также формировать условия для качественной, высокоэффективной защиты ценной информации.

Понятие информационной безопасности впервые было определено на теоретическом уровне с момента появления компьютерных технологий. В литературе отмечаются различные подходы к определению этого института: А.А. Стрельцов определяет информационную безопасность как невозможность нанесения вреда объектам безопасности, т.е. личности, обществу и государству, и она обуславливается защищённостью от различных угроз информационной безопасности. Также он отмечает, что достижение такого состояния защищённости, исключающего причинения вреда, достичь в принципе невозможно [1]. Более подробно понятие информационной безопасности раскрывает Р.Г. Яновский. Автор пишет, что информационная безопасность — это состояние, когда в обществе созданы все оптимальные условия, которые обеспечивают свободное развитие личности, семьи, государства, при этом данные условия дают возможность объективно оценить обстановку в мире, стране, регионе, вырабатывать самостоятельные решения на основе современной и достоверной информации [2].

Многие ученые поддерживают мнение, что информационная безопасность — это набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных в компьютерных сетях. В данном случае целью является обеспечение целостности информации, ее доступности [3]. Так, на современном этапе понятие информационной безопасности трактуется в различных подходах. Первый подход рассматривает определение информационной безопасности как комплекс мер по защите информации. Второй подход как обеспечение защиты от информационных воздействий и как комплекс мер по противодействию информационной войны. Третий подход рассматривает информационную безопасность как одну из составляющих во всех сферах жизнедеятельности, которая связана с производством, преобразование, потреблением, накоплением и хранением информации независимо от способов и средств осуществления этих процессов.

На законодательном уровне понятие информационной безопасности впервые было закреплено в 90-х годах 20 века в международных и национальных правовых актах. Закон «О безопасности» от 05.03.1992 № 2446–1 *(утратил силу)*, впервые закрепил термин «безопасность». В данном документе информационная безопасность была выделена в качестве одной из составляющих безопасности Российской Федерации. В утратившей силу «Доктрине информационной безопасности Российской Федерации» родовым признаком информационной безопасности являлось состояние защищенности национальных интересов России, а видовым то, что эти интересы определяются именно совокупностью сбалансированных интересов личности общества и государства.

В 1996 году был принят Федеральный закон «Об участии в международном информационном обмене» *(утратил силу)*. В данном нормативном правовом акте информационная безопасность понималась как состояние защищённости информационной среды общества, обеспечивающее её формирование и развитие в интересах граждан, организаций и государства.

Что касается международного закрепления информационной безопасности, то впервые понятие появилось в принятой по инициативе России 4 декабря 1998 года резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». В резолюции было отмечено, что информационные технологии и средства могут быть использованы не в целях совместимыми с задачами ООН.

В настоящее время информационная безопасность России — состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства [4]. Под информационными угрозами понимается совокупность действий и факторов, создающих опасность нарушения национальных интересов в информационной сфере. К ним относятся: рост применения информационных технологий, возрастание компьютерной преступности, рост иностранных организаций, осуществляющих техническую разведку в отношении России, и другие.

Объектами информационной безопасности являются личность, общество и государство. Информационная безопасность личности — это состояние человека, при котором ему не может быть нанесён существенный ущерб путём оказания воздействия на окружающее информационное пространство. Только малая часть населения имеет возможность защитить информацию, большая же часть нуждается в этой защите. В основе информационной безопасности общества лежит безопасность массового сознания граждан при наличии информационных угроз, в результате которой обостряется общественная психоэмоциональная напряжённость.

Информационная безопасность государства неразрывно связана с национальной безопасностью.

Важным документом в регулировании информационной безопасности является Доктрина информационной безопасности, которая представляет собой систему официальных взглядов на обеспечение национальной безопасности России в информационной сфере. Согласно Доктрине, национальными интересами в информационной сфере являются: обеспечение и защита прав и свобод человека и гражданина, развитие в России отрасли информационных технологий, обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, содействие формированию системы международной информационной безопасности. Угрозами информационной безопасности являются: наращивание зарубежными странами возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях; деятельность террористических и экстремистских организаций; компьютерная преступность, компьютерные атаки и другие. Доктрина информационной безопасности является частью законодательной системы Российской Федерации, в которой определены основы государственной политики, стратегия и тактика правового регулирования общественных отношений в сфере информационной безопасности [5] .

Для поддержания мировой стабильности и укрепления международных отношений необходимо обеспечивать международную информационную безопасность. Согласно Указу Президента РФ [6], который является документом стратегического планирования, основными угрозами международной информационной безопасности являются: использование информационно-коммуникационных технологий в экстремистских, преступных и террористических целях, в целях подрыва суверенитета, для посягательства на информационные ресурсы государства. Целями реализации государственной политики в сфере международной информационной безопасности являются предотвращение международных конфликтов в информационном пространстве и формирование системы обеспечения информационной безопасности на межгосударственном уровне. Данный Указ направлен на развитие сотрудничества государств в информационной сфере, совершенствование механизма обмена информацией, создание условий для обеспечения информационной безопасности, организацию международных конференций по вопросам противодействия использования информационных технологий в преступных целях.

Конвенция об обеспечении международной информационной безопасности (концепция) [7] устанавливает противодействие использованию информационно-коммуникационных технологий для нарушения международного мира и безопасности, а также меры, способствующие тому, чтобы деятельность государств в информационном пространстве способствовала общему социальному и экономическому развитию и осуществлялась таким образом, чтобы быть совместимой с задачами поддержания международного мира и безопасности.

Обеспечение информационной безопасности является важнейшей задачей Российской Федерации для противодействия угрозам безопасности личности, общества и государства. Обеспечение информационной безопасности — это осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Проблемами информационной безопасности можно считать утечку информации, кибервойну и кибертерроризм. Утечка информации — незаконное получение либо передача защищенных сведений (таких, как персональные данные, коммерческая, государственная тайна). В современном мире утечка информации окружает нас повсюду, хотя мы даже не догадываемся об этом. Возьмем, например, тот момент, когда нам регулярно звонят сотрудники банков, в которых мы не зарегистрированы. Встает вопрос: «Откуда им известны наши номера?». Всё элементарно. При обслуживании банковских карт в одном из банков, вся информация, полученная этим банком, размещается в общей базе, по сути, в открытом доступе, которая также может стать «жертвой» так называемых «хакеров». Также утечка информации по аналогичной схеме может происходить от компаний, занимающихся доставками. Один из примеров громкой утечки информации связан с компанией «Яндекс Еда» (сервис заказа быстрой доставки еды из ресторанов и продуктов из магазинов). В открытый доступ были представлены такие данные, как: имя, фамилия, контактный телефон, адрес поставки, комментарии и дата формирования заказа. По факту утечки данных «Яндекс.Еда» представила сообщение 1 марта 2022 года, в котором указано, что ситуация произошла из-за недобросовестных действий работника компании. Уже 22 марта в свободном доступе в сети Интернет появилась интерактивная карта с данными пользователей этого сервиса. В конце мая к этой информации подтянули сведения из реестров ГИБДД, СДЭК, Wildberries, «Билайн», ВТБ, «ВК» и ряда других фирм. Но в данном случае появление данных уже не было связано с утечкой информации. Правонарушители просто аккумулировали данные из различных источников. По стати-

стике ответственность за утечку информации лежит на сотруднике компании. Процесс отслеживание всех утечек данных в России возложен на Федеральную службу безопасности РФ. Для решения данной проблемы, по нашему мнению, необходимо усилить надзор в данной сфере, ввести отдельную меру ответственности для тех, кто «звонит», и для тех, откуда эта информация поступает.

Кибервойна. С сентября 2022 года, пока отношения России со странами Запада продолжают усложняться, все большую активность проявляют хакерские группировки. Стороны конфликта регулярно организуют DDoS-атаки на важные для оппонентов ресурсы и на время парализуют их работу. Как правило, хакеры хвастаются лишь моментальными результатами работы, например, тем, что тот или иной сайт временно прекратил работать. Именно поэтому вопрос о том, к каким последствиям на самом деле приводят их действия, остается открытым. До начала кибервойны ключевой целью хакеров обычно был шантаж компании-жертвы. Украв данные, они требовали у компании-жертвы выкуп и угрожали продать их третьим лицам, если не получат деньги. Однако после ухода крупных платежных систем из России для хакеров, которые объявили стране войну, эта задача перестала быть актуальной: теперь иностранные злоумышленники просто не могут воспользоваться номерами карт жителей страны. Однако в то же время в России активизировались внутренние хакеры: за последние месяцы количество оказавшихся в открытом доступе баз данных российских компаний выросло в два раза. При этом из междусобойчика российской группировки Killnet, выступившей на стороне России, и Anonymous, который на первых порах многими в даркнете воспринимался как самопиар и тех, и других, кибервойна превратилась в действительно огромное поле боя. От действий хакеров в итоге досталось и другим государствам, в их числе — страны Прибалтики, Молдавия, Италия, Япония и другие. Правозащитной функцией в данной сфере занимаются в совокупности практически все органы власти, в том числе: МВД РФ, ФСБ РФ, суды. Чтобы сократить угрозы, которые вызывают кибервойну, следует также усилить надзор в данной сфере, создав отдельное подразделение в органах исполнительной власти, например, при МВД РФ или ФСБ РФ. Также предлагается ужесточить меры ответственности в данной сфере.

Кибертерроризм — использование компьютерных и телекоммуникационных технологий (прежде всего, Интернет) в террористических целях. Самая скандальная кибератака на международном уровне произошла в мае 2020 года. Хакеры попытались взломать почтовые серверы Агентства национальной безопасности США. Злоумышленники использовали уязвимость в агенте пересылки сообщений Exim, обнаруженную в июне 2019 года. Она позволяет преступнику отправлять вредоносное письмо на сервер и сразу же получать возможность удаленно запускать там же свой код. АНБ обвинила в атаке хакерскую группировку Sandworm, связанную с Россией — ту самую, которая предположительно запустила вирус NotPetya. Ее же Минюст США позже обвинил в причастности к политическим событиям в Грузии и на Украине, а также во вмешательстве в выборы во Франции и атаке на компьютерную сеть Зимних Олимпийских игр в Пхенчхане в 2018 году. Также не стоит забывать о 2016 году, который принес много печальных новостей о подростках, существовании в социальных сетях некой игры «Синий кит», в которую играли дети и подростки, и финальной целью являлось совершение самоубийства.

Ключевыми организациями России, занимающимися вопросами безопасности в сфере кибертерроризма, являются: ФСБ РФ, Служба внешней разведки РФ, Министерство обороны РФ, Росгвардия, МВД РФ, Федеральная служба охраны РФ. 10 сентября 2020 года также стало известно о создании Генеральной прокуратурой РФ межведомственной рабочей группы для борьбы с киберпреступлениями. Кибертерроризм стоит признать глобальной проблемой и решать не только на уровне государства, но и совместно с другими странами на мировом уровне.

Организационное обеспечение информационной безопасности представляет собой совокупность различных мероприятий, направленных на защиту информации от несанкционированного доступа, планированию и использованию материальных, финансовых и иных ресурсов, а также управление ими, в целях противодействия угрозам информационной безопасности.

Государственная система информационной безопасности представляет собой совокупность органов государственной власти, осуществляющих обеспечение информационной безопасности. Органы государственной власти составляют организационную основу обеспечения информационной безопасности.

Так, Президент РФ осуществляет руководство органами по обеспечению информационной безопасности, определяет приоритетные направления в области государственной политики в области обеспечения информационной безопасности, утверждает Доктрину информационной безопасности, решает вопросы, связанные с обеспечением защиты информации и государственной тайны, заключает международные договоры в сфере обеспечения информационной безопасности. Федеральное Собрание РФ формируют законодательную базу в области защиты информации. Деятельность

Комитета Государственной Думы по информационной политике, информационным технологиям и связи направлена на законодательное регулирование в сфере информационных технологий и массовых коммуникаций, в том числе повышение эффективности государственного управления при обеспечении безопасности в информационном обществе. Правительство РФ участвует в определении основных направлений государственной политики в области обеспечения информационной безопасности; при формировании проекта федерального бюджета предусматривает выделение средств, которые необходимы для реализации федеральных программ в области информационной безопасности; организует исполнение законов по охране государственной тайны; устанавливает порядок разработки перечня сведений, составляющих государственную тайну; координирует деятельность органов государственной исполнительной власти.

Совет Безопасности РФ проводит стратегическую оценку состояния информационной безопасности России, рассматривает законопроекты об обеспечении информационной безопасности. В составе Совета Безопасности РФ функционирует межведомственная комиссия по информационной безопасности, которая создана в целях реализации задач, возложенных на Совет Безопасности в сфере обеспечения информационная безопасности. Данная комиссия анализирует состояние, прогнозирует, выявляет и оценивает угрозы информационной безопасности, рассматривает проекты федеральных целевых программ, направленные на обеспечение информационной безопасности.

Деятельность Федеральной службы по техническому и экспортному контролю РФ обеспечивает безопасность информации и объектов критической информационной инфраструктуры, выявляет угрозы информационной безопасности, осуществляет защиту государственной тайны, противодействует техническим разведкам. Федеральная служба безопасности России организует деятельность по борьбе с преступностью в информационной сфере, разрабатывает меры по защите сведений, составляющих государственную тайну, разрабатывает основные направления государственной политики в области международной информационной безопасности. Министерство внутренних дел РФ осуществляет борьбу с правонарушениями и преступлениями в информационной сфере. В структуре МВД создано специальное управление «К» для предотвращения и раскрытия компьютерных преступлений, преступлений, совершаемых с использованием информационно-телекоммуникационных сетей и направленных против здоровья несовершеннолетних, и общественной нравственности. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ осуществляет контроль и надзор в сфере связи, информационных технологий, защиты детей от информации, которая причиняет вред их здоровью.

Органами государственной власти осуществляется мониторинг потенциальных и реальных угроз информационной безопасности, вырабатывается повышенная устойчивость информационной инфраструктуры к их появлению. На современном этапе развивается система массовой достоверной информации для представления её гражданам и другим лицам, поскольку интерес о событиях общественной жизни внутри страны и за рубежом возрастает. Распространение массовой информации направлено на противодействие угрозам, нарушающим конституционные права граждан на свободное получение информации. Кроме того, формируется компетентность в области защиты информации детей, осуществляется сотрудничество органов власти, образовательных и дошкольных учреждений для повышения информационной культуры несовершеннолетних путём осуществления просветительских проектов. В области обеспечения информационной безопасности осуществляется лицензирование и сертификация данной деятельности. Лицензирование определяет право доступа конкретной организации к государственной тайне для выполнения работ и оказания услуг. Сертификация представляет деятельность по подтверждению соответствия средств защиты информации требованиям безопасности информации в целях защиты конфиденциальной информации.

Проблема обеспечения надлежащей безопасности персональной информации связана с тем, что в основном она собирается, обрабатывается и хранится коммерческими организациями. Соответственно, необходимо на уровне государства обеспечить контроль за соблюдением требований информационной безопасности данными организациями. Для чего необходимо определить все возможные риски и уязвимости, в соответствии с которыми разработать стандарты и правила их предотвращения и устранения.

Таким образом, по нашему мнению, решению проблем информационной безопасности России в настоящее время могут способствовать следующие мероприятия: дальнейшее развитие научно-практических основ информационной безопасности; формирование современной нормативно-правовой базы обеспечения информационной безопасности; ужесточение ответственности должностных лиц и граждан за нарушение требований информационной безопасности; разработка современных методов и технических средств, обеспечивающих комплексное решение задач защиты информации; укрепление технологической независимости России.

ЛИТЕРАТУРА

1. Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией А.А. Стрельцова.— Москва: Издательство Юрайт, 2021. 325 с.
2. Яновский Р.Г. Теоретические подходы в исследовании информационной безопасности // Информационная безопасность регионов. 2011. № 1 (8). С. 41–44.
3. Шободоева А.В. Развитие понятия «информационная безопасность» в научно-правовом поле России // Известия Байкальского государственного университета. 2017. № 1. С. 73–78.
4. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. 12.12.2016. № 50 ст. 7074.
5. Гриценко В.В. Доктрина информационной безопасности как политико-правовой документ стратегического планирования в сфере обеспечения национальной безопасности России // Правовая политика и правовая жизнь. 2017. № 2. С. 16–20.
6. Указ Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // Собрание законодательства РФ. 19.04.2021. № 16 (Часть I). ст. 2746.
7. Конвенция об обеспечении международной информационной безопасности (концепция) // МИД РФ [Электронный ресурс] URL: https://www.mid.ru/ru/foreign_policy/official_documents/1698725/ (дата обращения: 14.11.2022) .

Журнал «Современная наука: актуальные проблемы теории и практики»

Московский государственный юридический университет имени О.Е. Кутафина