ОГЛАВЛЕНИЕ

ГЛАВА 1

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЦИФРОВИЗАЦИЯ: ВЗАИМОВЛИЯНИЕ

§ 1. Понятие и содержание информационной безопасности в современных условиях

Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса с расширением использования современных информационных технологий эта зависимость усиливается. Значимость информационной безопасности для государства обусловлена тем, что информационная сфера обеспечивает функционирование всех остальных сфер жизни общества и от правильного определения соответствующих угроз зависит адекватный выбор средств защиты от них.

В Стратегии национальной безопасности Российской Федерации[7] развитие безопасного информационного пространства признано одним из национальных интересов Российской Федерации на современном этапе (п. 25), а информационная безопасность — стратегическим национальным приоритетом (п. 26).

В научной литературе и нормативных правовых актах понятие «безопасность» определяется по-разному применительно к различным

[7] СЗ РФ. 2021. № 27 (ч. II). Ст. 5351.

сферам, что обусловлено отличиями в подходах к исследованию столь многогранного явления. Множественность нормативно-правовых дефиниций безопасности (автомобиля, атомной станции, дорожного движения, биологической безопасности и еще около 30 видов объектов) и весьма противоречивых научных определений не в последнюю очередь обусловлена отсутствием легального определения термина «безопасность» в Федеральном законе от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[8]. В утратившем силу Законе РФ от 5 марта 1992 г. № 2446-1 «О безопасности»[9] под безопасностью понималось состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Характерно, что ни в одном, ни в другом законодательном акте информационная безопасность вообще не упоминалась.

Термин «безопасность» в российском законодательстве используется в двух смыслах: 1) состояние защищенности определенных объектов (субъектов); 2) свойство чего-либо, позволяющее обеспечивать защиту объектов в процессе использования, хранения и т.п.

Информационная безопасность в силу своей специфики также может рассматриваться и как состояние защищенности определенных субъектов (личность, общество, государство), и как свойство чего-либо (определенных объектов), позволяющее обеспечивать защиту (например, безопасность используемых технических средств). С этой точки зрения законодательство в сфере информационной безопасности образует два блока: 1) нормы, устанавливающие правовой режим информации, права, обязанности, ответственность субъектов информационных отношений, меры по созданию и обеспечению состояния информационной защищенности тех или иных объектов, формированию единой среды доверия; 2) нормы, устанавливающие требования к техническим средствам, сетям связи, условия передачи информации

[8] СЗ РФ. 2011. № 1. Ст. 2.
[9] Российская газета. 1992. № 103.

и т.п., что обусловливает их свойство обеспечивать защищенность информации и в конечном счете самих объектов.

В Стратегии национальной безопасности Российской Федерации национальная безопасность определена как состояние 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. Такая широкая трактовка позволяет говорить о том, что составной частью национальной безопасности является информационная безопасность.

Определенность в этот вопрос внес Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[10]. Согласно этому документу информационная безопасность Российской Федерации — это 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.

В некоторых нормативных правовых актах и публикациях речь идет о «безопасности информации». Это действительно важная составляющая информационной безопасности, но она не сводится исключительно к безопасности информации. В настоящее время с появлением новых технологий и новых угроз на первый план выдвигаются другие составляющие информационной безопасности — защищенность информации от несанкционированного доступа, от нарушения функционирования программно-технических средств ее сбора, обработки, накопления, хранения, поиска и передачи или от вывода

[10] СЗ РФ. 2016. № 50. Ст. 7074.

указанных средств из строя, обеспечиваемая совокупностью мер и средств защиты[11].

Проблемы обеспечения информационной безопасности существовали и ранее, не имея современного наименования и содержания и зачастую ограничиваясь военной тайной. Время, новые технологии, вызовы и угрозы меняют приоритеты, требования к информационной безопасности, что предполагает адекватное реагирование. Более того, меняется и объем, и состав информационной безопасности. При этом содержательно информационная безопасность одной группы субъектов может частично не совпадать с информационной безопасностью другой группы субъектов. Неслучайно в Доктрине информационной безопасности Российской Федерации речь идет о сбалансированных интересах личности, общества и государства в информационной сфере. Безопасность может различаться и внутри одной группы субъектов. Например, информационная безопасность личности взрослого человека содержательно не совпадает с информационной безопасностью детей и подростков[12].

На уровне отраслевого законодательства происходит конкретизация положений, касающихся информационной безопасности в определенной сфере с учетом существующих особенностей, что показано в отдельных параграфах настоящей работы (критическая информационная инфраструктура, медицина, образование, персональные данные и др.).

К основным информационным угрозам в компьютерных сетях, как правило, относят: «открытый доступ к вредоносной информации;

---

[11] См. ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения (утвержден приказом Ростехрегулирования от 29 декабря 2005 г. № 449-ст).

[12] Согласно Федеральному закону от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» информационная безопасность детей это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию (СЗ РФ. 2011. № 1. Ст. 48).

идеологическое загрязнение сетей; отсутствие барьеров; неконтролируемые контакты; недостаточность правовых знаний о работе с информацией, авторском праве и др.»[13].

Обеспечение и защита национальных интересов Российской Федерации неразрывно связаны с информационной безопасностью как одним из стратегических национальных приоритетов. Стратегия национальной безопасности Российской Федерации к одному из главных национальных интересов относит развитие безопасного информационного пространства, защиту российского общества от деструктивного информационно-психологического воздействия. Это направление играет все более важную роль в отношении как государства, так и личности, поскольку дезинформация, деструктивное информационно-психологическое воздействие, манипулирование человеческим сознанием (определенного сообщества, группы, национальности) применяются все шире, становятся одним из основных приемов, с помощью которых ежедневно оказывается влияние на человека (чаще — на определенное сообщество) и его поведение. Используется множество различных технологий, позволяющих управлять людьми и их сознанием[14], в том числе путем распространения недостоверной информации.

В психологии под манипуляцией массовым сознанием (общественным мнением) понимается способ управления большим количеством людей (сообществами) путем создания иллюзий и условий для управления их поведением. Манипуляция — один из основных способов информационной войны (прежде всего, на международном уровне), задача которой — установить контроль над поведением людей, направить его в требуемом направлении посредством изменения представлений, мнений, побуждений и целей. Полагаем, что на эффективность

---

[13] Гришина Т.М. Обеспечение безопасности российского бизнеса в сетевом обществе: некоторые правовые вопросы // Безопасность бизнеса. 2017. № 4. С. 3–8.

[14] См., например: Чалдини Р. Психология влияния. М., 2018; Экман П. Психология лжи. 4-е изд. / пер. с англ. СПб., 2010; Райгородский Д.Я. Психология масс: хрестоматия. Самара, 1998.

манипулирования массовым сознанием в значительной степени влияет уровень образованности человека и его общей культуры.

Активное развитие и внедрение во все сферы жизни ИКТ сопровождаются появлением новых угроз безопасности граждан, общества и государства, активизацией уже существующих угроз. В Стратегии национальной безопасности Российской Федерации отмечается, что происходит расширение использования ИКТ для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности. Это не только деструктивное информационно-психологическое влияние, но и прямое воздействие на различные объекты инфраструктуры, банковский сектор, государственные информационные системы путем осуществления хакерских атак, распространения недостоверной информации, заведомо ложных сообщений, призывов к массовым беспорядкам, осуществлению экстремистской деятельности и т.п.

Так, по данным «Ростелеком-Солар», в 2022 г. на российские компании было совершено 911 тыс. хакерских атак, что вдвое больше, чем годом ранее[15]. Более того, эксперты предполагали дальнейший рост количества кибератак на российские компании. По их мнению, число инцидентов должно увеличиться минимум на 50%[16].

Исследователи отмечают, что «вектор атак сместился в сторону от нарушения целостности, доступности и конфиденциальности информации к деструктивным воздействиям на компоненты технологической инфраструктуры, нарушающим корректность ее функционирования»[17].

В отношении государственного сектора ситуация еще более серьезная — число кибератак в 2022 г. выросло в три раза. Такие атаки

---

15 По состоянию на 20 февраля 2023 г. (www.rbk.ru).

16 URL: https://www.rbc.ru/technology_and_media/13/10/2022/6346cdcc9a7947891c7fd5fc

17 Лаврова Д.С., Зегжда Д.П., Зайцева Е.А. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. 2019. № 2 (30). С. 13.

затрагивают интересы и граждан, и коммерческих структур. Так, кибератака в апреле 2023 г. на информационную систему таможенных органов по всей стране парализовала таможенное оформление грузов. В результате сбоя в единой информационной системе таможенных органов (далее — ЕАИС ТО) на два дня были остановлены все процедуры таможенного оформления в России. Подать декларации на товары как в электронном, так и в бумажном виде было невозможно, электронный документооборот отсутствовал[18]. В связи с подобными ситуациями высказывается мнение, что в настоящее время нецелесообразно полностью исключать бумажную форму делопроизводства и документооборота.

Вместе с ростом количества кибератак эксперты отмечают в государственном секторе и рост утечек конфиденциальной информации. Это тоже одна из угроз информационной безопасности — прежде всего, личности. Так, в 2022 г. количество утечек выросло, по мнению экспертов, в три раза по сравнению с 2021 г. В сети «Интернет» регулярно обнаруживаются базы данных как коммерческих структур (прежде всего, банков), так и российских органов государственной власти. Среди них наиболее часто называют Главный радиочастотный центр, Министерство культуры РФ, ФНС России и др.[19] Произошла утечка данных о ковидных больных. Было заявлено, что эти данные будут уничтожаться через пять недель после того, как человек выздоровел, но этого не было сделано. В результате сведения о 300 тыс. пациентов оказались в продаже на хакерском форуме[20].

Следует учитывать, что любая информационная система уязвима. Пока еще не создано системы, которую нельзя было бы взломать. По мнению Н. Касперской, различия хорошо и плохо защищенной системы только в количестве ресурсов, которые злоумышленнику необходимо потратить на взлом. С этой точки зрения системы, содержащие

---

18 Коммерсантъ. 2023. № 63.

19 Там же.

20 URL: https://aif.ru/society/web/pochemu_mask_ne_da_vinchi_kasperskaya_-_o_cifrovom_kontrole_i_kloune_iz_ssha

биометрические данные, иные ценные сведения, наиболее привлекательны для кибератак.

По мнению специалистов в области информационной безопасности, «…цифровые документы гораздо больше, чем бумажные, подвержены утечке, краже, искажению, компрометации. Это создает принципиально новые типы массового мошенничества (фишинг, веерные звонки "от службы безопасности вашего банка" и др.). Известны случаи массовых мошенничеств с недвижимостью путем подделки цифровых кадастров и реестров» [21].

Положительным моментом является усиление внимания к информационной безопасности как в государственном, так и в частном секторе. Роскомнадзор, который отвечает за кибербезопасность российского сегмента сети «Интернет», сообщил, что в 2022 г. злоумышленники неоднократно атаковали портал «Госуслуги», однако все атаки прошли «без ущерба»[22].

Одним из условий обеспечения информационной безопасности является формирование безопасной среды оборота достоверной информации, единой цифровой среды доверия. Снижение рисков и угроз информационной безопасности, повышение уровня защищенности — задачи постоянные, которые приходится решать с учетом развития и использования новых технологий, расширения сфер применения электронных документов, включения широкого круга участников электронного взаимодействия в различные по характеру отношения.

Нарушение информационной безопасности может быть связано не только с умышленным совершением правонарушений, преступных деяний в информационной сфере, но и с организацией электронного взаимодействия, передачей, хранением электронных документов, сложностью установления, от кого поступил тот или иной электронный документ, действительно ли в нем выражена воля лица, нет ли

[21] URL: https://aif.ru/society/web/pochemu_mask_ne_da_vinchi_kasperskaya_-_o_cifrovom_kontrole_i_kloune_iz_ssha

[22] Там же.

в нем изменений. И здесь встает вопрос о доверии, о формировании пространства доверия.

Принципиальное значение для формирования единой цифровой среды доверия имеют такие меры, предусмотренные Национальной программой «Цифровая экономика Российской Федерации» в части формирования единой цифровой среды доверия, как создание единой системы идентификации и аутентификации (ЕСИА)[23] и введение в правовое поле биометрической идентификации, позволяющие с достоверностью установить личность человека, вступающего в конкретные отношения, его правовой статус, другую необходимую информацию. В свою очередь, это позволяет в том числе сформировать юридически значимый электронный документооборот.

Единая цифровая среда доверия должна обеспечивать возможность совершения юридически значимых действий в электронной форме, позволяя убедиться в том, что мы имеем дело с конкретным субъектом, что направленное нами сообщение и полученное нами от этого субъекта сообщение имеют неизмененное содержание. Соответственно, единая цифровая среда доверия должна создавать условия:

а) для достоверного подтверждения личности (идентификация, аутентификация);

б) подтверждения достоверности и неизменности электронных документов.

Создание единой цифровой среды доверия невозможно обеспечить исключительно техническими методами. Без законодательного решения это неосуществимо, равно как и применение для идентификации исключительно правовых методов вряд ли окажется эффективным.

Не менее значимыми для формирования единой цифровой среды доверия являются проблемы, связанные с электронным документом. В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, утвержденной Указом Президента РФ от

[23] Однако эта система пока далеко не полная и не охватывает все население Российской Федерации.

9 мая 2017 г. № 203[24], в числе основных направлений указаны продвижение проектов по внедрению электронного документооборота в государственном и частном секторе, создание условий для повышения доверия к электронным документам.

На повышение доверия к электронным документам направлены изменения, внесенные в Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» Федеральным законом от 27 декабря 2019 г. № 476-ФЗ. В частности, введен новый субъект — доверенная третья сторона, осуществляющая деятельность по проверке электронной подписи в электронных документах в конкретный момент времени в отношении лица, подписавшего электронный документ, для обеспечения доверия при обмене данными и электронными документами и иные функции, предусмотренные Федеральным законом «Об электронной подписи».

Наряду с подтверждением действительности электронных подписей доверенная третья сторона проверяет соответствие квалификационных сертификатов, задействованных при подписании электронного документа, установленным требованиям, полномочия участников электронного взаимодействия, а также создает и проверяет метку доверенного времени и др.

В ходе интеграционных процессов важно обеспечить формирование единой цифровой среды доверия не только в границах Российской Федерации, но и значительно шире — в рамках Евразийского экономического союза (далее — ЕАЭС). Соответственно, задача формирования единой цифровой среды доверия расширяется до формирования трансграничного пространства доверия.

Правовое обеспечение формирования трансграничного пространства доверия создается более активно, чем российское национальное законодательство по тем же вопросам. В ЕАЭС по данным вопросам принято более 60 документов. Под трансграничным пространством

[24] Официальный интернет-портал правовой информации: http://www.pravo.gov.ru

доверия в соответствии с Договором о Евразийском экономическом союзе (далее — Договор о ЕАЭС)[25] понимается совокупность правовых, организационных и технических условий, согласованных государствами-членами с целью обеспечения доверия при межгосударственном обмене данными, и имеющих юридическую силу электронных документов между субъектами электронного взаимодействия при реализации общих процессов в рамках Союза с использованием системы, обеспечивающей интеграцию территориально распределенных государственных информационных ресурсов и информационных систем уполномоченных органов государств-членов, а также информационных ресурсов и информационных систем Евразийской экономической комиссии (далее — ЕЭК).

В целях формирования трансграничного пространства доверия принята Стратегия развития трансграничного пространства доверия[26], в которой определены основные цели, задачи и принципы развития трансграничного пространства доверия для использования сервисов и имеющих юридическую силу электронных документов при межгосударственном информационном взаимодействии государств — членов ЕАЭС, а также приоритеты развития институционального, правового, организационного и технического обеспечения трансграничного пространства доверия.

Право на доступ к информации, его реализация — неотъемлемая составная часть информационной безопасности как личности, так и государственных и негосударственных структур. Границы права на доступ к информации подвижны, при этом в настоящее время они имеют два прямо противоположных вектора развития: на расширение права на доступ к информации и на ограничение доступа к

---

[25] Договор подписан в г. Астане 29 мая 2014 г. (ред. от 8 мая 2015 г., с изм. и доп., вступ. в силу с 12 августа 2017 г.) (официальный сайт ЕЭК: http://www.eurasiancommission.org/).

[26] См.: Решение коллегии ЕЭК от 27 сентября 2016 г. № 105 «О Стратегии развития трансграничного пространства доверия» (начало действия документа — 9 января 2019 г.) // СПС «КонсультантПлюс».

определенным видам информации. И тот и другой тесно связаны и обусловлены процессом цифровизации.

Современные информационные технологии облегчают и расширяют доступ к информации, в том числе путем ее предоставления государственными органами и органами местного самоуправления неограниченному кругу лиц посредством ее размещения в сети «Интернет» в форме открытых данных и свободного (бесплатного) использования. Существенную роль в расширения доступа к информации призваны сыграть государственные информационные системы (ГИС). Расширению права на доступ к информации могут способствовать и организационные меры, принимаемые не только государством, но и коммерческими структурами.

Направления ограничения права на доступ к информации и ее распространение, так же как и на его расширение, во многом связаны с использованием современных информационных технологий, прежде всего сети «Интернет». Ограничение права на распространение определенной информации в социальных сетях и мессенджерах это, как правило, требование государства (государственных органов) в отношении запрещенной законом информации или информации, для которой установлен режим ограниченного доступа, направленное на обеспечение информационной безопасности государства, населения, личности. Чрезвычайно важным и знаковым представляется новое явление, когда ограничения на доступ и распространение информации исходят не от государства, а от негосударственных структур. По сути это ограничения, не установленные законом, но от этого не менее действенные.

Принципиально новым направлением ограничения доступа к информации стало изменение круга лиц, принимающих решение об ограничении доступа к информации. Это не государство, а владельцы крупных социальных сетей, самостоятельно определяющие свою политику, в том числе по доступу к информации, ее распространению. Наиболее громкий пример такого ограничения, ставший известным

всему миру, это блокирование возможности высказать свое мнение в социальных сетях действующему на тот момент Президенту США Д. Трампу.

Такие действия близки по сути к цензуре. В связи с этим возникает вопрос о том, что понимается под цензурой в настоящее время и кто ее осуществляет. По общему правилу это контроль за содержанием и распространением информации, характерными чертами которого являются предварительный характер его осуществления публичными органами власти. Конституция РФ и в ее развитие Закон РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»[27] запрещают только предварительную цензуру и только публичными органами власти.

В комментарии к указанному закону отмечается, что ограничения свободы слова и информации должны иметь властный и императивный характер[28]. Принципиальное значение для признания конкретного требования цензурой имеет статус вынесшего его субъекта. Однако в современных условиях возможность запретить или ограничить доступ к той или иной информации, ее распространение появляется и у других субъектов при одновременном ослаблении контрольной функции государства. По сути это тоже цензура, но не государственная, что не меняет ее сущности как ограничителя доступа к информации, но уже по усмотрению владельцев социальных и иных сетей. В ряде стран, например в Германии, введены официальные требования к владельцам социальных сетей осуществлять контроль за размещаемой в этих сетях информацией.

Возможность ограничить доступ к определенной информации принадлежит и человеку. Во многих странах, в том числе и в России, наряду с традиционными правами на личную, семейную тайну, тайну частной жизни было признано право на забвение, которое позволяет

---

[27] Ведомости СНД и ВС РФ. 1992. № 7. Ст. 300.

[28] См.: Жеребцов А.Н., Ротко С.В., Рыдченко К.Д. и др. Комментарий к Закону РФ от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации» // СПС «КонсультантПлюс».

человеку ограничить доступ к информации о нем. Это право — одно из самых новых прав, и появилось оно как обеспечение информационной безопасности личности, как ответ на новое состояние информации, когда Интернет «все помнит». Все публикации, любая информация, однажды попавшие во Всемирную сеть, будут храниться практически вечно. Право на забвение, предоставленное человеку, позволяет прервать неограниченный доступ и неограниченное существование конкретной информации об этом человеке.

Следует отметить, что информационная безопасность не является неизменной величиной: с бурным развитием современных информационных технологий появляются новые виды угроз, на которые необходима быстрая и адекватная реакция. Появляются и активно проникают в жизнь новые виды вредной информации, отрицательно влияющие на состояние информационной безопасности, такие как треш-стримы, фейки и т.д., а сама проблема информационной безопасности выходит за рамки одного государства и становится международной проблемой, приобретает трансграничный характер[29]. Неслучайно международная информационная безопасность стала предметом регулирования в Основах государственной политики Российской Федерации в области международной информационной безопасности, утвержденных Указом Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности».

К настоящему времени в мире сформировалась определенная система взглядов на проблему обеспечения безопасности информационно-телекоммуникационной инфраструктуры, информационных систем, которые становятся наиболее уязвимыми областями национальной безопасности. Вывод из строя любого существенного элемента

[29] См.: Полякова Т.А., Смирнов А.А. Правовое обеспечение международной информационной безопасности: проблемы и перспективы // Российский юридический журнал. 2022. № 3. С. 7–15.

информационной инфраструктуры может привести к невосполнимому ущербу и катастрофическим последствиям.

Безопасность информации как важная составляющая информационной безопасности включает в себя:

– защиту информации и информационных ресурсов от несанкционированного доступа, искажения, уничтожения, модифицирования, блокирования;

– установление режима информации в зависимости от ее содержания;

– обеспечение защиты сведений, составляющих государственную тайну, иную информацию ограниченного доступа.

На обеспечение информационной безопасности направлена и программа импортозамещения продукции сферы информационных технологий. Так, с 1 января 2016 г. вступило в силу постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд». Указанным постановлением установлен запрет на допуск программ для ЭВМ и баз данных (реализуемых независимо от вида договора — на материальном носителе и (или) в электронном виде по каналам связи), происходящих из иностранных государств, а также исключительных прав на такое программное обеспечение (далее — ПО) и прав использования такого ПО в целях осуществления закупок для обеспечения государственных и муниципальных нужд. По общему правилу заказчики обязаны ограничить закупки в основном российским ПО. При этом российским признается ПО, сведения о котором внесены в единый реестр российских программ для ЭВМ и баз данных.

Представляет интерес проведенный С.А. Авакьяном анализ направлений опасностей в информационной сфере. Он отмечает, что «добившись конституционных и в целом нормативных гарантий права на информацию, на ее создание и распространение, на владение

информацией, тем более права на защиту информации, мы сталкиваемся с повальной необходимостью защиты ОТ информации», наглядно показывая, что «свобода информации очень быстро продемонстрировала свою обратную сторону — возможность проявления неуважения к личности, неуправляемое заимствование и распространение частных (персональных) данных, а тем более лжи и клеветы, беззащитность человека»[30].

Действительно под видом свободы слова зачастую создается и распространяется общественно вредная, недостоверная информации, в том числе такая, как фейки и треш-стримы. Относительно фейков целесообразно привести еще одну позицию, изложенную С.А. Авакьяном. Он совершенно справедливо обращает внимание на огромную роль информации в формировании публичных настроений, особенно в настоящее время, когда ведется информационная война против российского народа[31].

Внимание государства к проблеме умышленного распространения недостоверной информации многократно возросло в связи с широким использованием Интернета различными слоями населения, причем она носит общемировой характер, поэтому государства ищут оптимальные пути ее решения[32]. Фейковой стали называть не только

---

[30] Авакьян С.А. Задачи конституционного права в аспекте защиты (от) информации // Конституционное и муниципальное право. 2022. № 8. С. 3–11.

[31] Там же.

[32] Так, Закон Филиппин 2017 г. «О злонамеренном распространении ложных сведений и других связанных с этим нарушениях» определяет ложную информацию как информацию, вызывающую панику, хаос, разногласия, насилие или ненависть, а также информацию, содержащую элементы пропаганды с целью очернить или дискредитировать человека. Согласно Закону Сингапура 2019 г. «О защите от распространения в Интернете фейковой информации и манипуляций» устанавливается уголовная ответственность за публикацию фейковых новостей. В Германии действует Закон 2017 г. Net Enforcement Act (NetzDG). Малайзийский закон Anti-fake news Act 2018 г. предусматривает наказание как за инициацию ложной информации, так и за репосты; fake news — любые новости, информация, сведения и отчеты, которые являются полностью или частично ложными независимо от формата (журнальная, газетная статья; телевизионная программа, видео- или аудиозапись; иной формат, способный передавать слова и мысли) (см.: Щербаков А.Д. Fake news как объект уголовно-правовой регуляции: опыт Малайзии //

информацию, это относится и к сайтам, похожим до смешения с официальными, куда, как правило, предлагается перевести деньги за уплату штрафа.

Одновременно с определением в Федеральном законе «Об информации, информационных технологиях и о защите информации» понятия «недостоверная общественно значимая информация» был принят Федеральный закон от 18 марта 2019 г. № 27-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[33]. Статья 13.15 «Злоупотребление свободой массовой информации» КоАП РФ дополнена ч. 9–11, согласно которым распространение информации, создавшее угрозу причинения вреда жизни и здоровью граждан, имуществу, угрозу массовых беспорядков, угрозу нарушения функционирования объектов жизнеобеспечения, влечет наложение административного штрафа. Новеллы относительно фейковой информации были включены в указанную статью, тем самым показана их связь со средствами массовой информации (далее — СМИ).

Уголовный кодекс РФ также включает в себя новеллу, которой установлено, что преступлением является «публичное распространение под видом достоверных сообщений заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, и (или) о принимаемых мерах по обеспечению безопасности населения и территорий, приемах и способах защиты от указанных обстоятельств…». Таким образом, УК РФ не содержит указания на способ публичного распространения фейковой информации, главное условие — это публичное распространение.

Верховный Суд РФ обращает внимание на то, что в рамках уголовной ответственности публичный характер распространения

Международное уголовное право и международная юстиция. 2018. № 4. С. 18–21; Ильяшенко А.Н., Хисамова З.И. О некоторых аспектах привлечения к уголовной ответственности за распространение fake news в социальных сетях в условиях пандемии // Российский следователь. 2020. № 9. С. 12–15).

[33] СЗ РФ. 2019. № 12. Ст. 1217.

заведомо ложной информации может проявляться не только в использовании для этого СМИ и информационно-телекоммуникационных сетей, но и в распространении такой информации путем выступления на собрании, митинге, при раздаче листовок, вывешивании плакатов и т.п.

Фейк — это объект, который представляет интерес для многих стран, причем связан он с двумя прямо противоположными возможностями его проявления и использования. С одной стороны, это борьба с фейками и дезинформацией, нарушающими информационную безопасность населения, самого государства; с другой — возможность государства осуществлять информационную войну в отношении других стран, вбрасывать в информационное поле, прежде всего в социальные сети, дезинформацию.

Принципиальное отличие недостоверной информации от фейков — это субъективное отношение к их созданию. Фейковая информация создается умышленно и распространяется сознательно с целью введения в заблуждение. Необходимо отметить, что широкому распространению фейков, на наш взгляд, способствует низкий уровень медиаграмотности населения и общей культуры в целом.

В настоящее время имеет место фундаментальная зависимость национальных компьютерных сетей, инфраструктуры России от зарубежных технологий, что обусловило возникновение новых угроз, которые связаны, прежде всего, с возможностью использования ИКТ в целях, несовместимых с национальными интересами.

Одним из направлений решения проблем безопасности является интенсификация развития отечественного производства аппаратных и программных средств защиты информации и методов контроля за их эффективностью, 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.

Факторы уязвимости России в информационной сфере определяются наличием таких серьезных проблем, как технологическая зависимость от иностранных государств в сфере информатики, недостаточный уровень защищенности критически важных сегментов информационной инфраструктуры и низкая степень государственного контроля ее внутреннего информационного пространства.

По мере включения новых технологий в жизнь общества возникают и новые проблемы информационной безопасности, причем далеко не всегда опасные стороны этих новых технологий очевидны. Так, например, определенные угрозы несет интернет вещей. Но пока данные технологии не заняли значительного места в нашей жизни, и скрытые опасности пока не исследованы.

§ 2. Векторы развития института информационной безопасности в условиях цифровизации

Вопросы формирования новой правовой модели информационной безопасности в условиях цифровизации и цифровой трансформации общественных отношений в настоящее время становятся предметом научных исследований[34].

Определение такой модели основывается на трех направлениях, в рамках которых институционализируются соответствующие конкретные векторы развития правового регулирования информационной безопасности, — это стратегическое планирование, международно-правовое регулирование и внутригосударственное (национальное) регулирование.

---

[34] См.: Терещенко Л.К., Зырянов С.М. Правовая модель информационной безопасности в Российской Федерации: структура и ключевые параметры // Вестник Московского университета МВД России. 2019. № 5. С. 226–230.

Стратегия национальной безопасности Российской Федерации, утвержденная Указом Президента РФ от 2 июля 2021 г. № 400, установила, что целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве.

Достижение данной цели в соответствии со Стратегией осуществляется путем реализации государственной политики, направленной на решение следующих задач:

1) формирование безопасной среды оборота достоверной информации, повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования;

2) развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз;

3) предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры Российской Федерации;

4) создание условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием ИКТ;

5) повышение защищенности и устойчивости функционирования единой сети электросвязи Российской Федерации, российского сегмента сети «Интернет», иных значимых объектов информационно-коммуникационной инфраструктуры, а также недопущение иностранного контроля за их функционированием;

6) снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений установленных российским законодательством требований по защите такой информации и персональных данных;

7) предотвращение и (или) минимизация ущерба национальной безопасности, связанного с осуществлением иностранными государствами технической разведки;

8) обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий;

9) укрепление информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов, а также разработчиков и изготовителей вооружения, военной и специальной техники;

10) развитие сил и средств информационного противоборства;

11) противодействие использованию информационной инфраструктуры Российской Федерации экстремистскими и террористическими организациями, специальными службами и пропагандистскими структурами иностранных государств для осуществления деструктивного информационного воздействия на граждан и общество;

12) совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии ИИ и квантовые вычисления;

13) обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности, в том числе при реализации национальных проектов (программ) и решении задач в области цифровизации экономики и государственного управления;

14) укрепление сотрудничества Российской Федерации с иностранными партнерами в области обеспечения информационной безопасности, в том числе в целях установления международно-правового режима обеспечения безопасности в сфере использования ИКТ;

15) доведение до российской и международной общественности достоверной информации о внутренней и внешней политике Российской Федерации;

16) развитие взаимодействия органов публичной власти, институтов гражданского общества и организаций при осуществлении деятельности в области обеспечения информационной безопасности Российской Федерации.

Решение данных задач на уровне стратегического планирования требует соответствующей актуализации и обеспечения системной взаимосвязи иных документов стратегического планирования в сфере информационных отношений, в их числе:

– Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы (Указ Президента РФ от 9 мая 2017 г. № 203);

– Стратегия научно-технологического развития Российской Федерации (Указ Президента РФ от 1 декабря 2016 г. № 642);

– Стратегия развития отрасли информационных технологий в Российской Федерации на 2014–2020 годы и на перспективу до 2025 года (распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р);

– Стратегия развития электронной промышленности Российской Федерации на период до 2030 года (распоряжение Правительства РФ от 17 января 2020 г. № 20-р);

– План мероприятий (дорожная карта) «Создание дополнительных условий для развития отрасли информационных технологий» (утвержден Правительством РФ 9 сентября 2021 г.);

– Единый план по достижению национальных целей развития Российской Федерации на период до 2024 года и на плановый период до 2030 года (утвержден Правительством РФ 1 октября 2021 г.).

Кроме того, в соответствии с Перечнем поручений Президента Российской Федерации по итогам заседания Совета по стратегическому развитию и национальным проектам от 18 июля 2022 г. № Пр-1553 (подп. «и» п. 1) разработана и утверждена Концепция технологического развития Российской Федерации на период до 2030 года (распоряжение Правительства РФ от 20 мая 2023 г. № 1315-р), в которой в качестве одной из угроз обозначены проблемы информационной безопасности Российской Федерации.

Также при развитии стратегического планирования в сфере обеспечения информационной безопасности должны учитываться положения новой Концепции внешней политики Российской Федерации, утвержденной Указом Президента РФ от 31 марта 2023 г. № 229. В соответствии с данной Концепцией к национальным интересам Российской Федерации во внешнеполитической сфере отнесены развитие безопасного информационного пространства и защита российского общества от деструктивного иностранного информационно-психологического воздействия. При этом достижение стратегических целей внешней политики Российской Федерации осуществляется путем выполнения ряда задач, в числе которых формирование объективного восприятия России за рубежом, укрепление ее позиций в мировом информационном пространстве.

Согласно Концепции в целях обеспечения международной информационной безопасности, противодействия угрозам в ее отношении, укрепления российского суверенитета в глобальном информационном пространстве Российская Федерация намерена уделять приоритетное внимание:

1) укреплению и совершенствованию международно-правового режима предотвращения и разрешения межгосударственных конфликтов и регулирования деятельности в глобальном информационном пространстве;

2) формированию и совершенствованию международно-правовых основ противодействия использованию ИКТ в преступных целях;

3) обеспечению безопасного и стабильного функционирования и развития информационно-телекоммуникационной сети «Интернет» на основе равноправного участия государств в управлении данной сетью и недопущению установления иностранного контроля над ее национальными сегментами;

4) принятию политико-дипломатических и иных мер, направленных на противодействие политике недружественных государств по милитаризации глобального информационного пространства,

по использованию ИКТ для вмешательства во внутренние дела государств и в военных целях, а также по ограничению доступа других государств к передовым ИКТ и усилению их технологической зависимости.

На международно-правовом уровне в рамках развития института международной информационной безопасности необходимо учитывать общие вызовы и перспективы международно-правового регулирования общественных отношений, векторы международно-правового регулирования самого института информационной безопасности, а также перспективы международного развития российской модели международной информационной безопасности.

К общим вызовам и перспективам международно-правового регулирования общественных отношений в информационной сфере следует отнести проблему обеспечения суверенитета и навязывания моделей правового регулирования недружественных стран и международных организаций (цифровой неоколониализм)[35].

Кроме того, к международно-правовым вызовам относятся и вопросы правового регулирования локализации данных, осуществляемой в рамках национального законодательства отдельных государств, и как следствие — фрагментация мирового информационного пространства (киберпространства). При этом альтернативой политики локализации и фрагментации может являться опережающее развитие и экспорт российских информационных технологий, а также моделей их правового регулирования.

Сложность решения этих задач обусловлена и множественностью площадок для разработки регулирования (Группа правительственных экспертов ООН, Рабочая группа открытого состава ООН, Международный союз электросвязи, Шанхайская организация сотрудничества (далее — ШОС), ЕАЭС.

---

[35] См.: Ефремов А.А. Государственный суверенитет в условиях цифровой трансформации // Правоведение. 2019. Т. 63. № 1. С. 47–61.