УДК 34.096

Петренко М.Н.
кандидат юридических наук, соискатель
Саратовская государственная юридическая академия
ORCID: 0000-0002-0046-6754
Россия, г. Москва

К ВОПРОСУ О ДИФФЕРЕНЦИАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ В ОТЕЧЕСТВЕННОМ ЗАКОНОДАТЕЛЬСТВЕ

Аннотация. *В условиях перехода отечественного общества к постиндустриальному (цифровому) этапу развития, в настоящий момент обособляемому агрессивной и противоправной деятельностью ряда стран т.н. коллективного Запада, значимую роль играет обеспечение безопасности, в особенности – информационной. Произошедший 19.07.2024 крупнейший сбой в функционировании программного обеспечения, повлекший заметные проблемы в транспортной, банковской и иных сферах деятельности многих стран мира акцентировал её актуальность. В статье предпринята попытка с практических позиций рассмотреть вопрос целесообразности существующего многообразия классификаций информационных систем, содержащихся в регламентирующих вопросы информационной безопасности нормативно-правовых актах, а также обосновывается возможность сокращения неактуальных дифференциаций для повышения эффективности правового регулирования. В итоге это может способствовать совершенствованию правового базиса отечественной информационной безопасности. В рамках исследования использовалась совокупность методов, основными из которых являлись логический, формально-юридический, сравнительно-правовой методы.*

Ключевые слова: *нормативное регулирование, информационная безопасность, государственная информационная система, муниципальная информационная система, критическая информационная инфраструктура, информационная система персональных данных*.

Annotation: *In the context of the transition of domestic society to the post–industrial (digital) stage of development, currently isolated by the aggressive and illegal activities of a number of countries of the so-called collective West, an important role is played by ensuring security, especially information security. The largest software malfunction that occurred on 07/19/2024, which caused noticeable problems in transport, banking and other spheres of activity in many countries of the world, emphasized its relevance. The article attempts to consider from a practical point of view the expediency of the existing variety of classifications of information systems contained in regulatory legal acts regulating information security issues, and also substantiates the possibility of reducing irrelevant differentiations to improve the effectiveness of legal regulation. As a result, this can contribute to improving the legal basis of domestic information security. The study used a set of methods, the main of which were logical, formal legal, comparative legal methods.*

Key words: *regulation, information security, state information system, municipal information system, critical information infrastructure, personal data information system.*

Вероятно ни у кого в современном обществе не вызывает сомнений необходимость информационной защищённости базисных сведений о жизни граждан и функционировании государства, в том числе обеспечение недоступности сведений о состоянии здоровья человека, опасном и оборонном производстве, транспорте и связи, о банковских и иных финансовых системах (а также, вероятно, в ряде иных сфер) посторонним лицам.

Практически это объясняется продуцируемым быстрым развитием и распространением информационно-коммуникационных технологий (далее – **ИТТ**) повышением вероятности использования последних в противоправной деятельности,[1] а также детерминируемым усложнением технологических систем ухудшением их отказоустойчивости. С точки зрения теории права основой сложившейся ситуации является «формирование новой группы прав человека – цифровых прав, осуществление которых связано с использованием информации, представленной в цифровой форме»,[2] обусловленной переходом к постиндустриальному (информационному) этапу развития общества.

Произошедший 19.07.2024 глобальный сбой в функционировании одной из наиболее распространенных на настоящий момент операционных систем в очередной раз показал уязвимость жителей многих стран мира перед современными информационными угрозами: на значительное время исчезли возможности получения медицинской помощи, использования транспорта и финансовых инструментов. Жители многих стран были (а, вероятно, и будут) вынуждены тратить свое время, силы, средства на преодоление иных негативных последствий произошедшего инцидента. Причем подобное понимание событий сложно списать на искусственное «сгущение красок» в отношении стран Запада, поскольку даже The Guardian (которую едва ли можно назвать придерживающейся пророссийской направленности) в статье «‘Largest IT outage in history’ hits Microsoft Windows and causes global chaos», прямо именует произошедшее крупнейшим сбоем в работе информационно-телекоммуникационных технологических систем.[3]

Следует отметить, что несмотря на сложности, порожденные указанным сбоем во многих странах мира, Россию указанные события сколько-нибудь заметно не затронули (несмотря, а скорее всего – благодаря развитости как бытового, так и промышленного использования ИТТ). Такой результат является закономерным итогом заблаговременно принятых органами власти

мер по обеспечению информационной безопасности (далее – **ИБ**), сформированных на основании дальновидно принятой Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 05.12.2016 № 646.[4] Принятые меры, и это свершившийся факт, позволили защитить Российскую Федерацию и её жителей от последствий на настоящий момент крупнейшего в мире информационно-телекоммуникационного сбоя.

Вместе с тем, прогресс в сфере ИТТ не стоит на месте, и то, что вчера оказалось достаточным, уже сегодня может стать малоэффективным, а завтра – бессмысленным. В сфере ИБ высокая интенсивность развития отрасли требует постоянного поиска и внедрения лучших, по сравнению с существующими, решений. Причем не только в технологических вопросах, но и в нормативной регламентации, которые совместно с мерами организационными являются фундаментальной основой защиты информации.[5]

Одной из проблем правового обеспечения ИБ, вполне способной иметь существенные негативные последствия, является вопрос многообразия, вероятно избыточного, существующих в законодательстве классификаций информационных систем, именуемых нами в дальнейшем нормативными классификациями информационных систем.

Так, частью 1 статьи 13 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон № 149-ФЗ) определено, что информационные системы (далее – **ИС**) подразделяются на государственные (федеральные и региональные), муниципальные и иные ИС.[1] Законодатель вполне буквально разграничивает государственные и муниципальные ИС, посвящая им даже отдельные пункты (1 и 2) приведенной части статьи, дифференцируя их в зависимости от субъекта принятия решения о создании системы: если решение отражено в федеральных законах, законах субъектов Российской Федерации,

в правовых актах государственных органов – ИС государственная, если же решение закреплено в решениях органа местного самоуправления – ИС муниципальная.

Действительно, на первый взгляд масштаб информационных систем государственного (даже регионального) и муниципального уровня не сопоставим. Вопросы местного значения в целом схожи для различных уровней местного самоуправления и включают в себя сугубо локальные вопросы: например, установление местных налогов, дорожная деятельность, содействие развитию народных промыслов,[2] что, кажется, не может таить в себе чего-то существенного, требующего особенной, специальной защиты. От того, на первый взгляд, муниципальные ИС ввиду малозначительности содержащихся в них данных не требуют объёмной и развитой системы защиты информации, необходимой для государственных ИС.

Вместе с тем, реализация полномочий по разрешению вопросов местного значения требует от муниципалитетов обработки различной информации, и в весьма значительных объемах. Так, в силу части 1 статьи 4 Федерального закона от 20.08.2004 № 113-ФЗ «О присяжных заседателях федеральных судов общей юрисдикции в Российской Федерации» исполнительно-распорядительный орган муниципального образования каждые четыре года составляет список и запасной список кандидатов в присяжные заседатели муниципального образования, включая в указанные списки граждан, постоянно проживающих на территории соответствующего муниципального образования.[3] Частью 6 статьи 17 Федерального закона от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» определено, что сведения об избирателях, участниках референдума формирует и уточняет глава местной администрации муниципального района, муниципального округа, городского округа, внутригородской территории города федерального значения, а в случаях, предусмотренных законом субъекта Российской

Федерации - города федерального значения, - руководитель территориального органа исполнительной власти города федерального значения.[4]

Таким образом муниципалитеты хранят и иным образом, так или иначе, обрабатывает данные в отношении всех своих жителей, включая сведения о специальном статусе отдельных из них – например, статусе кандидата в присяжные заседатели. Сложно всерьез усомниться в том, что утрата, повреждение, подмена такой информации может иметь негативные последствия как для отдельных лиц, чьи данные могут быть использованы, например, для совершения мошенничества в отношении них или их близких, так и для общества в целом, например, в связи с манипуляциями при составлении коллегии присяжных заседателей.

Разграничение ИС на государственные и муниципальные нашло отражение в ведомственных нормативных правовых актах в области ИБ, в частности – в Требованиях о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Пунктом 3 указанных требований установлено, что последние являются обязательными при обработке информации в государственных информационных системах, функционирующих на территории Российской Федерации, а также в муниципальных информационных системах, если иное не установлено законодательством Российской Федерации о местном самоуправлении.[5] Иными словами, несмотря на заложенное в федеральном законе разграничение приведенных видов информационных систем, в подзаконном нормотворчестве указанные категории практически отождествляются для целей единообразия регламентации, хотя и сохраняя за муниципальными ИС возможность индивидуализации в регулировании при особых обстоятельствах.

Думается, в нынешних условиях необходимо дальнейшее развитие инициативы Федеральной службы по техническому и экспортному контролю России по сближению (а в итоге, вероятно, – отождествлению)

государственных и муниципальных ИС. Это объясняется не только отмеченной выше сравнимой значимостью данных, обрабатываемых в указанных ИС, а также необходимостью защиты информации на высоком уровне. Для принятия указанного решения уже сформирована и нормативная основа.

Так, в конце 2020 года принят Федеральный закон «О Государственном Совете Российской Федерации», статьей 2 которого установлено, что под органами публичной власти понимаются федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, иные государственные органы, органы местного самоуправления в их совокупности.[6] Справедливо полагать, что применительно к обеспечению безопасности ИС вполне подходящим является именно этот правовой конструкт – ИС органов публичной власти. Основные доводы в защиту предлагаемого подхода можно означить следующим образом.

Во-первых, симплификация нормативного регулирования способствует самостоятельному совершению необходимых для обеспечения безопасности действий, а следовательно – улучшению уровня информационной безопасности при одновременном сокращении необходимости внешнего властного вмешательства.

Во-вторых, унификация нормативных требований в сфере информационной безопасности способствует качественному улучшению формы и содержания нормативных правовых актов.[7]

В-третьих, объективизация нормативного регулирования в сфере информационной безопасности за счет приведения «нормативного» в соответствие с «объективным» (закрепление фактически существующего повышенного уровня безопасности муниципальных ИС), как и унификация, потворствует улучшению качественных характеристик правового регулирования.

В-четвертых, актуализация нормативной регламентации вопросов информационной безопасности путем приведения её в соответствие с существующими нормативными конструктами обновляет существующие правовые связи, и совместно с объективизацией сокращает существующие между ними расхождения.

Ввиду изложенного в краткосрочной перспективе развитие нормативного регулирования в сфере ИТТ видится, в том числе, за счет исключения бинарности нормативного регулирования для государственных и муниципальных ИС путем объединения предъявляемых к ним требований как к ИС органов публичной власти.

Оценивая среднесрочную перспективу следует отметить, что «многие исследователи, отмечающие различные аспекты несовершенства информационного законодательства, убеждены в целесообразности его систематизации для устранения данных противоречий путем кодификации законодательства в данной сфере, которое должно идти параллельно с процессом нормотворчества».[8] Следует признать что указанный подход способствовал бы гармонизации нормативной регламентации в сфере ИБ, в том числе за счет сокращения используемых для установления различных правовых режимов функционирования ИС выделяемых законодателем видов ИС. Значительное число последних, вероятно, усложняет и ухудшает понимание требований ИБ на практике, что неизбежно ведет к невыполнению или неполному / неверному выполнению существующих законодательных требований в рассматриваемой сфере.

Так, например, помимо указанной выше содержащейся в законодательстве классификации ИС на государственные (федеральные и региональные), муниципальные и иные, законодатель также предлагает рассматривать ИС как относящиеся (вне зависимости от отнесенности к какой-либо категории значимости либо признания его незначимым) и не относящиеся к объектам критической информационной инфраструктуры,[9]

относящихся и не относящихся к информационным системам персональных данных (вне зависимости от необходимых уровней защищенности и типов присущих угроз).[10] У всех приведенных видов ИС в основе находится различный признак: субъект – у первой, значимость ИС – у второй и содержание информационной системы – у третьей классификации. При этом информационная система может одновременно являться, например, государственной и при этом обрабатывать персональные данные (особенности регулирования такого рода систем закреплены в статье 13 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [11]). Таким образом законодателем признается существование различных комбинаций видов ИС, влекущих неизбежные трудности сочетания различных, предусмотренных для каждого отдельного их вида, законодательных требований. Это несомненно усложняет понимание нормативной регламентации правоприменителями.

Вместе с тем приведенное усложнение в сфере обеспечения государственной безопасности, частью которой является безопасность информационная, в текущих условиях роста внешних вызовов едва ли уместно.

Как сказано ранее, государственные и муниципальные ИС точнее, а на современном этапе государственного строительства – ещё и более обоснованно, именовать ИС органов публичной власти. Однако ретроспективная оценка указанной дифференциации свидетельствует о том, что смысл выделения законодателем государственных и муниципальных ИС заключается в установлении для них повышенных, по сравнению с иными системами, требований к ИБ. Иными словами квинтэссенция указанной классификации та же, что и у более позднего Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» (и основанных на нем подзаконных актах) - структуризация ИС в зависимости от их важности на 4 категории: от 0 до 3. С рассматриваемых

позиций разница между лишь в том, что последний разграничивает ИС не в зависимости от субъектов (что было вполне уместно и обоснованно на первоначальных этапах создания правовой базы ИБ), но по иным критериям: сфере функционирования ИС, значимости ИС и ряду других.[12] На первое место встает содержание системы, а не её владелец.

При таком рассмотрении нормативная (но, подчеркнем, не доктринальная) [13] дифференциация ИС в зависимости от субъекта предстаёт в значительном смысле утратившей актуальность, поскольку объективно не столь важно, кто является субъектом критической информационной инфраструктуры – государство, муниципалитет, частная коммерческая или не коммерческая организация. Если в системе обрабатывается социально, политически, экономически, научно или по иным критериям значимая информация – она должна быть защищена, в том числе для обеспечения консолидированной государственной безопасности. И чем более значима обрабатываемая информация – тем больший уровень безопасности должен нормативно предусматриваться и обеспечиваться для указанной ИС (в пользу указанного подхода свидетельствует и то, что несмотря на несомненную значимость сведений, обрабатываемых в ИС органов публичной власти, среди них обязательно найдутся и те, которые обрабатывают утратившие актуальность, а от того не значимые в настоящее время, сведения. Либо системы, созданные в качестве формальности и изначально не включающие в себя сколько-нибудь важных сведений. С другой стороны, не вызывает сомнений и тот факт, что сведения, обрабатываемые не в государственной, а, например, в ИС корпораций Росатом, Ростех, государственных внебюджетных фондов, не заслуживают автоматического отнесения к малозначимым лишь на том основании, что субъектом выступают коммерческие или некоммерческие организации).

Важным видится использование для установления требований к субъектам ИС возможно и сложной, но единой (построенной на единых

принципах, правилах и др.) классификации ИС. Устойчивой основой для неё, как это отмечено выше, может послужить ранее разработанный органами власти подход к дифференциации ИС, нашедший отражение в законодательстве об объектах критической информационной инфраструктуры.

Изложенное приводит к выводу, что отвечающее вызовам современности развитие нормативной классификации ИС на среднесрочную перспективу видится в дальнейшем совершенствовании концепции отечественного законодательства об объектах критической информационной инфраструктуры в ранее заложенном законодателем русле, заключающейся в дифференциации ИС в зависимости от значимости обрабатываемых сведений и независимо от субъекта. В краткосрочной перспективе уместным явилось бы объединение государственных и муниципальных ИС в нормативных правовых актах под единым наименованием – ИС органов публичной власти.

В совокупности принимаемые меры могли бы способствовать укреплению информационной защищенности граждан, общества и государства, тем самым усовершенствовав действующую систему обеспечения государственной безопасности Российской Федерации.

Использованные источники:

1. Подробнее: Данилов Д. Ю., Бут Н. Д. Защита критической информационной инфраструктуры средствами прокурорского надзора как важная составляющая национальной безопасности // Вестник Университета прокуратуры Российской Федерации. — 2024. — № 2 (100). — С. 45-52.

2. Туликов А. В. Информационная безопасность и права человека в условиях постиндустриального развития (теоретико-правовой анализ) : автореф. дисс. на соиск. уч. степ. канд. юрид. наук. — М., 2017. — С. 8.

3. «Largest IT outage in history» hits Microsoft Windows and causes global chaos // The Guardian. — 2024. — 19 июля. — URL: https://www.theguardian.com/australia-news/article/2024/jul/19/microsoft-windows-pcs-outage-blue-screen-of-death (date: 19.07.2024).

4. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации. — 2016. — 50. — ст. 7074.

5. часть 1 статьи 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации. — 2006. — № 31 (1 ч.). — ст. 3448).

6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. — 2006. — № 31 (1 ч.). — ст. 3448.

7. Федеральный закон от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» // Собрание законодательства Российской Федерации. — 2003. — № 40. — ст. 3822.

8. Федеральный закон от 20.08.2004 № 113-ФЗ «О присяжных заседателях федеральных судов общей юрисдикции в Российской Федерации» // Собрание законодательства Российской Федерации. — 2004. — № 34. — ст. 3528.

9. Федеральный закон от 12.06.2002 № 67-ФЗ «Об основных гарантиях избирательных прав и права на участие в референдуме граждан Российской Федерации» // Собрание законодательства Российской Федерации. — 2002. — № 24. — ст. 2253.

10. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Российская газета. — 2013. — 26 июня. — № 136.

11. Федеральный закон от 08.12.2020 № 394-ФЗ «О Государственном Совете Российской Федерации» // Собрание законодательства Российской Федерации. — 2020. — № 50 (ч.3). — ст. 8039.

12. Подробнее: Стрюков Е. А. К вопросу об условиях и направлениях унификации нормативных правовых актов // Пробелы в российском законодательстве. — 2014. — №2. — URL: https://cyberleninka.ru/article/n/k-voprosu-ob-usloviyah-i-napravleniyah-unifikatsii-tormativny h-pravovyh-aktov (дата обращения: 23.07.2024).

13. Вепренцева Т. А. Актуальные проблемы правового обеспечения информационной безопасности РФ // Национальная безопасность. — 2022. — №2. URL: https://cyberleninka.ru/article/n/aktualnye-problemy-pravovogo-obespecheniya-informatsionnoy -bezopasnosti-rf (дата обращения: 28.07.2024).

14. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации. — 2017. — № 31 (ч.1). — ст. 4736.

15.Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // Собрание законодательства Российской Федерации. — 2012. — № 45. — ст. 6257.

16. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. — 2006. — № 31. (ч.1) — ст. 3541.

17. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // Собрание законодательства Российской Федерации. — 2018. — № 8. — ст. 1204.

18. Бояринцева О.А. Государственных и муниципальные (публичные) базы данных как объекты информационных правоотношений : автореф. дисс. на соиск. уч. степ. канд. юрид. наук. — М., 2019. — С. 14.