ПРАВОВЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

УДК 34.01:004 DOI 10.37468/2307-1400-2024-2-42-65

ОТЕЧЕСТВЕННЫЙ И МИРОВОЙ ОПЫТ ГАРМОНИЗАЦИИ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Метельков Александр Николаевич [1]
Александрова Алена Юрьевна [1]

[1] Санкт-Петербургский университет Государственной противопожарной службы МЧС России имени Героя Российской Федерации генерала армии Е.Н. Зиничева, Санкт-Петербург, Россия

АННОТАЦИЯ

Целью статьи является анализ отечественного и зарубежного опыта (на критическом анализе опыта США) в сфере гармонизации правового регулирования защиты информации. В последние годы приобретает актуальность и необходимость исследование гармонизации подходов, понятий в сфере обеспечения информационной безопасности, которая государством названа в числе основных приоритетов национальной безопасности. В науке гармонизация рассматривается на межведомственном, внутригосударственном, межгосударственном, международном и других уровнях. Общераспространенным в юридическом мире в контексте гармонизации является подход к рассмотрению приоритета над национальным правом международных норм, ратифицированных государством. Однако это вовсе не означает, что такой приоритет показывает прямое действие достигнутых международных соглашений. Очевидно, международное право устанавливает лишь общие направления социально-экономического развития, а национальные государства реализуют их посредством суверенной национальной правовой политики и совершенствования нормативной правовой базы. В результате проведенного исследования, на примере МЧС России, сформулированы предложения по гармонизации некоторых основных терминов в сфере обеспечения безопасности информации.

Ключевые слова: гармонизация, информационная безопасность, защита информации, правовое регулирование.

DOMESTIC AND INTERNATIONAL EXPERIENCE IN HARMONIZING REGULATORY LEGAL ACTS IN THE FIELD OF INFORMATION SECURITY

Metelkov Alexander N. [1]
Alexandrova AlenaYu. [1]

[1] *St. Petersburg University of the State Fire Service of EMERCOM of Russia named after Hero of the Russian Federation Army General E.N. Zinichev, St. Petersburg, Russia*

ABSTRACT

The purpose of the article is to analyze domestic and foreign experience (using the example of the USA) in the field of harmonization of legal regulation of information protection. In recent years, it has become urgent and necessary to study the harmonization of approaches and concepts in the field of information security, which the state has named among the main priorities of national security. In science, harmonization is considered at interdepartmental, intra-state, interstate, international and other levels. A common approach in the legal world in the context of harmonization is to consider the priority of international norms ratified by the State over national law. However, this does not mean that such a priority shows the direct effect of the international agreements reached. Obviously, international law establishes only general directions of socio-economic development, and national States implement them through a sovereign national legal policy and improvement of the regulatory legal framework. As a result of the conducted research, using the example of the Russian Ministry of Emergency Situations, proposals were formulated for the harmonization of some basic terms in the field of information security.

Keywords: harmonization, information security, information protection, legal regulation.

Введение

С момента осуществления социально-политических преобразований в Российской Федерации начала 1990-х годов в условиях масштабного обновления всех сторон общественного и государственного бытия, сопровождающегося порой противоречивостью и непоследовательностью реформ, объектом пристального научного анализа, с неуклонно возрастающим вниманием со стороны правотворческой и правоприменительной практики, становится гармонизация российского законодательства [1, с.3]. Поэтому справедливо утверждение Ю.А. Тихомирова, что «на передний план выдвигается стратегическая задача гармонизации правовых актов» [2, с.238]. При рассмотрении понятийного аппарата в сфере обеспечения конфиденциальности информации Г.Г. Камалова в докторской диссертации, отметила, что конфиденциальность как свойство информации ограниченного доступа, посвящена анализу соотношения взаимосвязанных понятий. Выявлено отсутствие в законодательстве нормдефиниций большинства анализируемых понятий («конфиденциальность информации», «информация ограниченного доступа», «тайна» и «секрет», «секретная», «конфиденциальная» информация, «неприкосновенность», «негласность» и т.д.) и единства взглядов ученых на используемую терминологию [3, с.26].

Информационно-телекоммуникационные технологии стали одним из наиболее важных факторов, влияющих на формирование общества XXI века. Развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства. Увеличивается количество компьютерных атак на российские информационные ресурсы. Большая часть таких атак осуществляется с территорий иностранных государств. Инициативы Российской Федерации в области обеспечения международной информационной безопасности встречают противодействие со стороны иностранных государств, стремящихся доминировать в глобальном информационном пространстве [4]. Бурные темпы развития и распространения информационных технологий, в условиях реальных угроз проведения тайных кибероперациий в информационном пространстве в военно-политических и иных целях, обострение конкурентной борьбы и криминогенной обстановки требуют создания целостной системы информационной безопасности, взаимоувязывающей правовые, оперативные, технологические, организационные, технические и физические меры защиты информации на гармонизированной терминологической базе.

Система ООН в силу своих, в настоящее время достаточно ограниченных возможностей, способствовала развитию международного сотрудничества, что отразилось и на юридических аспектах процессов гармонизации, и в некоторых аспектах унификации международно-правового регулирования правовых в информационной сфере. Принимая во внимание отражение государственного суверенитета в публично-правовых отраслях внутригосударственного права развитию подобных процессов препятствует их активная политизация. Несмотря на осложнение выработки коллективных ответов на транснациональные вызовы и угрозы, такие как использование информационно-коммуникационных технологий в противоправных целях и международный терроризм в силу объективных противоречивых процессов глобализации гармонизация и унификация в сфере российского информационного права возможна с учетом отдельных конструктивных подходов, апробированных в развитых странах.

Как вполне справедливо утверждает А.С. Минзов, методологическое обеспечение информационной безопасности находится в постоянном развитии, что «проявляется в неоднозначности подходов к интерпретации отдельных терминов, неопределенностью методологических подходов к моделированию угроз, уязвимостей и информационных рисков, а также в отсутствии формализаций и стандартов для описания процессов защиты информации и сценариев атак» [5, с.45].

Процесс развития права под воздействием глобализации в юридической литературе обозначается термином «интернационализация» или

«гомогенизация». Содержание данного явления состоит в распространении общепризнанных принципов, норм и иных положений международного права на национальное право государств, в сближении нормативного содержания национального права отдельных стран, в учете иностранной составляющей в механизме правового регулирования внутренних общественных отношений и т.п. Правовыми инструментами данного процесса являются гармонизация, унификация, рецепция, имплементация и стандартизация. Термин «гармонизация законодательства» обычно означает приведение национальной нормативной правовой базы в соответствие с требованиями международного права для устранения правовых коллизий и обеспечения единообразной интерпретации законов в процессе вступления государства в экономические или политические союзы.

Гармонизация предопределяется зависимостью государств друг от друга в вопросах технологического развития. Доктриной информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646, в информационную сферу включены сети связи. Сети связи являются частью российской информационной инфраструктуры, играющей важную роль в реализации стратегических национальных приоритетов нашей страны. Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры и единой сети электросвязи Российской Федерации в мирное и военное время являются национальными интересами в информационной сфере. Одной из основных угроз информационной безопасности назван высокий уровень зависимости отечественной промышленности от зарубежных информационных технологий в части программного обеспечения, вычислительной техники и средств связи, что обуславливает распределение между государствами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет»[6,с. 26].

Теоретические взгляды на гармонизацию имеют определенное не всегда совпадающие подходы. Академиком РАН Т.Я. Хабриевой в статье «Гармонизация правовой системы РФ в условиях международной интеграции: вызовы современности» (2014) отмечается возможность высокой степени правовой гармонизации в рамках однородных правовых сообществ и семей. В праве гармонизацию исследуют с использованием горизонтального и вертикального подходов. Правоведы нередко рассматривают гармонизацию как правовой институт. Л.П. Рассказов, например, определяет термин «гармонизация» как норму «интернационализации, направленную на обеспечение совместимости национального права с международным правом и в определенной степени с правом других государств» [7, с. 534]. Гармонизация, по его мнению, «предполагает согласование национального права с правом международным и правом других государств посредством изменения, дополнения и принятия национальных нормативных правовых актов или посредством их исключения из правовой системы»[7, с. 534]. Гармонизация в информационном праве осложняется бурным развитием новых информационных технологий и утратой актуальности «старых», что отражается в национальном праве на техническом регулировании в информационной сфере.

Еще в 1990-х годах ряд государств осознал негативный аспект неконтролируемого использования информационно-телекоммуникационных технологий в международных отношениях. Однако, как отмечает А.Я. Капустин, «продвижение вперед в создании международно-правового механизма противодействия угрозам информационной безопасности особо не ощущается, он так и не сформирован…» [8, с.45-46]. В декабре 2021 г. Генассамблея ООН без голосования приняла совместную резолюцию России и США о нормах поведения в киберпространстве «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий». Россия и США призвали не допускать применения информационных ресурсов или технологий «в преступных

или террористических целях». Соавторами резолюции о нормах поведения в киберпространстве стали Австралия, Соединённое Королевство, Франция, Германия и др. Также Россия и США пригласили все страны присоединиться к этим правилам поведения в киберпространстве.

Право на информацию, ограниченно признанное на этапе становления конституционного государства, в условиях формирования информационного общества приобретает новое значение. Право на доступ к информации, требующее от государства дополнительного регулирования и определения механизма доступа, то есть позитивных действий, повлияло на пересмотр отношения к природе права на информацию [9, с.17].

Проблемы гармонизации на опыте США

Стремление политических кругов США и транснациональных корпораций закрепить свое монопольное положение в сети «Интернет» и контролировать все информационные ресурсы сопровождается навязыванием своих взглядов на цифровую трансформацию и блокировкой развития альтернативных интернет-платформ. В результате с учетом накопленного опыта и результатов освоения современных информационных технологий США в интересах однополюсной глобализации пользователям глобальной сети навязывается свои стандарты, которые необходимо критически учитывать в гармонизации российского понятийно-терминологического аппарата в сфере информационной безопасности.

Возможность гармонизации политики кибербезопасности в 2024 г. находится в центре внимания Министерства внутренней безопасности США (DHS) и Европейской комиссии, которые объявили об инициативе по сотрудничеству в согласовании требований к отчетности о киберинцидентах. Эти усилия на высоком уровне, возглавляемые Р. Сильверсом, заместителем министра по стратегии, политики и планов Министерства внутренней безопасности, и Р. Виолой, генеральным директором DG Connect Европейской комиссии, предоставляют возможность гармонизировать важные элементы кибербезопасности экосистемы между трансатлантическими экономиками. Гармонизация способствует созданию более безопасной цифровой экосистемы (цель, которую разделяют правительства и промышленность), давая компаниям уверенность в том, что их инвестиции в исследования и разработки более эффективных решений безопасности будут соответствовать требованиям правительств и, в конечном итоге, достигнут рынка. Гармонизация законов и политики помогает правительствам на международном уровне, поскольку облегчает координацию, укрепляет международное партнерство и способствует инновациям и торговле. В заявлении Министерства национальной безопасности и Европейской комиссии упоминается совместный отчет, в котором определены шесть областей для сравнения, включая определения, пороговые значения, сроки и основное содержание отчетов.

Глобальная киберповестка Альянса программного обеспечения (BSA) на 2024 год отражает приоритеты сектора корпоративных технологий в области кибербезопасности. В ней содержится настоятельный призыв к тому, чтобы политика строилась на успешной основе государственно-частного партнерства, подходов, основанных на учете рисков, и международнопризнанных стандартов и передовой практики. BSA рекомендует использовать искусственный интеллект для улучшения безопасной разработки программного обеспечения и улучшения управления рисками кибербезопасности. В повестке дня BSA на 2024 г. описаны рекомендации, которые правительствам следует расставить по приоритетам для обеспечения наибольших достижений в области кибербезопасности, с акцентом на следующих ключевых темах: повышение безопасности программного обеспечения; улучшение управления рисками кибербезопасности; инвестиции в современные информационные технологии, а также гармонизация законов и политики в области кибербезопасности. Таким образом, BSA определило гармонизацию как императив. Эта работа соответствует и отражает приоритеты, изложенные в BSA

«Глобальная киберповестка дня на 2024 год», в которой подчеркиваются преимущества гармонизации внутри правительств и между правительствами. Гармонизация является приоритетом для Глобальной программы кибербезопасности, поскольку посредством гармонизированных законов и политик, основанных на международнопризнанных стандартах и передовом опыте, можно повысить безопасность всей цифровой экосистемы.

Важность этого решения заключается в том, что гармонизация представляет собой возможность повысить уровень кибербезопасности для всех взаимодействующих субъектов и объектов. Гармонизированные законы и политика внутри правительства облегчают координацию между ведомствами.

В США в последнее время наиболее остро, в аспекте гармонизации, встал вопрос в отношении киберинцидентов. Из-за отсутствия унификации отчетности об инцидентах в США – и вытекающих из этого негативных последствий – Конгресс создал Совет по отчетности о киберинцидентах на основании Закона о критической инфраструктуре. Это помогло подготовить отчет DHS «Гармонизация отчетности о киберинцидентах перед федеральным правительством». В частности, в США существует множество проблем, связанных с согласованием свыше 45 действующих федеральных требований к отчетности о киберинцидентах. Существенные различия между действующими требованиями к сообщению об инцидентах часто обусловлены различными соображениями национальной и экономической безопасности в различных секторах критически важной инфраструктуры, а также различными интересами правительства в области защиты потребителей и инвесторов. К числу наиболее серьезных проблем, связанных с гармонизацией, относятся различия в определениях, сроках и механизмах представления отчетности, содержании отчетов, требований и механизмах отчетности. Кроме того, существуют процессуальные и ресурсные проблемы, а также юридические препятствия для согласования.

Существенной проблемой для согласования текущих и будущих требований федерального правительства к отчетности о киберинцидентах является существенное различие между самими режимами. Центр реагирования на киберинциденты (CIRC) проанализировал действующие и предлагаемые режимы отчетности о киберинцидентах, чтобы выявить общие черты и расхождения. Основываясь на этой оценке и обсуждениях с соответствующими заинтересованными сторонами, DHS определило несколько областей, в которых различия между режимами являются наиболее обременительными для организаций, которые должны отчитываться перед несколькими ведомствами. Проблемными, с точки зрения гармонизации, были названы различия в определениях киберинцидентов, о которых можно сообщать. Многие из этих различий являются функциями различных правительственных целей, стимулирующих различные режимы отчетности о киберинцидентах, которые могут отражать различия в оперативных последствиях, экономических последствиях (например, с точки зрения цепочки поставок) и конфиденциальности. Связь между целью режима и конкретными требованиями наиболее очевидна, когда речь заходит о сроках представления отчетности и содержании отчетов.

Режимы, ориентированные на потенциальную национальную, экономическую и общественную безопасность, скорее всего, будут иметь более короткие сроки представления отчетности, чем режимы, ориентированные на неприкосновенность частной жизни и защиты прав потребителей. Устанавливается порядок киберинцидентов, о которых можно сообщать, и пороговые значения для отчетности. Тип информации об инциденте – воздействие на сервисы, первопричина, характер вредоносной активности и т.д. – также определяется ответственностью запрашивающего агентства и целью режима отчетности.

В существующих нормативных актах используются различные формулировки для определения киберинцидентов, о которых можно сообщать, или иного описания порога того, о чем можно

сообщать. Существующие определения и пороговые значения и те, которые будут предложены в будущих нормативных документах, необходимо будет учитывать в рамках будущих усилий по гармонизации. Одним из ключевых отличий существующих режимов является то, как они характеризуют последствия инцидентов, о которых необходимо сообщать. Режимы отчетности о киберинцидентах и соответствующие законодательные органы, как правило, используют ряд терминов, таких как «существенные потери», «сбои» и «серьезные последствия», для описания пороговых значений инцидентов, о которых необходимо сообщать. Каждое из этих пороговых значений предполагает некоторое ощутимое воздействие, прежде чем потребуется отчетность, но все они могут по-разному интерпретироваться для определения соответствующего воздействия. Другие ведомства определяют простое присутствие или даже подозрение на присутствие вредоносного кода или несанкционированной активности как инцидент, о котором можно сообщить. Примеры различных определений и пороговых значений включают:

– киберинцидент, который приводит к существенной потере конфиденциальности, целостности или доступности такой информационной системы или сети, или к серьезному снижению безопасности и отказоустойчивости операционных систем и процессов (Закон США «Об Отчетности о киберинцидентах для критической инфраструктуры», 2022 г., CIRCIA, раздел 2242);

– инцидент кибербезопасности означает событие, которое без законного разрешения ставит под угрозу, нарушает работу или иным образом воздействует или с разумной вероятностью может поставить под угрозу, нарушить работу или иным образом повлиять на целостность, конфиденциальность или доступность компьютеров, информационных или коммуникационных систем или сетей, физической или виртуальной инфраструктуры, контролируемой компьютерами или информационными системами, или информация, хранящаяся в системе (Управление транспортной безопасности США –TSA, Директива по безопасности 1582-21-01);

– киберинцидент означает действия, предпринятые с использованием компьютерных сетей, которые приводят к компрометации или фактическое или потенциально неблагоприятное воздействие на информационную систему и/или содержащуюся в ней информацию или на способность подрядчика выполнять требования контракта, которые определены как критически важные с точки зрения оперативной поддержки (Министерство обороны – DoD, DFARS 252.204-7012).

Кроме этого, существует несогласованность в режимах отчетности об инцидентах в отношении того, считаются ли инциденты, которые все еще находятся на стадии внутреннего расследования, киберинцидентами, о которых можно сообщать. Например, у TSA в это определение явно включены расследуемые киберинциденты. Решение TSA о включение расследуемых киберинцидентов было обусловлено потенциальным каскадным воздействием на другие важнейшие секторы инфраструктуры. Это определение включает событие, которое расследуется или оценивается владельцем (оператором) в качестве возможного инцидента кибербезопасности без окончательного определения первопричины или характера события (например, вредоносного, подозрительного, доброкачественного) (Директива по безопасности 1580/82-2022-01). Другие агентства исключают из определения инцидентов, о которых следует сообщать, те потенциальные инциденты, которые были эффективно смягчены защитными мерами или внедрением передовых методов обеспечения кибербезопасности и, таким образом, не привели к несанкционированным взломам. Например, недопустимое использование или раскрытие защищенной медицинской информации считается нарушением, если только юридическое лицо или деловой партнер, на которых распространяется действие, не продемонстрирует, что существует низкая вероятность того, что защищенная медицинская информация была скомпрометирована, основываясь на оценке риска (Министерство здравоохранения и социального обеспечения США –HHS, Правило уведомления о нарушениях

HIPAA 45 C.F.R 164.400-414).

Другой вопрос, непосредственно связанный с целью режима отчетности, заключается в том, является ли несанкционированный доступ или раскрытие персональных данных инцидентом, о котором можно сообщить. Такое раскрытие информации лежит в основе отчетности в рамках различных режимов HHS и FTC, но не обязательно охватывается режимами в других критически важных секторах инфраструктуры, где основное внимание уделяется инцидентам, которые могут привести к сбоям в работе при поставке товаров или услуг.

Различные временные рамки и механизмы подачи сообщений о киберинцидентах также представляют серьезную проблему для гармонизации отчетности. Сроки представления отчетности для режимов национальной или экономической безопасности варьируются от «немедленно» (FHFA и SEC в определенных случаях) или «незамедлительно» (CFTC, SEC в определенных случаях, Министерство юстиции и программа CISA по антитеррористическим стандартам на химических объектах) до «одного часа» (DOE) или «72 часов» (CIRCIA и Министерство обороны), или просто «без задержки» (USCG). Напротив, большинство сроков подачи сообщений о нарушениях конфиденциальности и защиты прав потребителей варьируются от 7 рабочих дней с момента обоснованного выявления нарушения, в соответствии с правилом CPNIFCC о нарушении данных, до 10 дней, в соответствии с правилом FTC об уведомлении о нарушениях в сфере здравоохранения. Для организаций, на которые распространяется действие HIPAA, срок уведомления составляет 60 дней с момента обнаружения нарушения или до конца календарного года. Межведомственное руководство по программам реагирования для организаций, на которые распространяется действие HIPAA, является исключением из требований, касающихся конфиденциальности и защиты прав потребителей. Несанкционированный доступ к информации о клиентах и уведомление клиентов предусматривают, что учреждение должно иметь процедуры для уведомления своего главного федерального регулирующего органа «как можно скорее». Существуют также «многоуровневые» сроки представления отчетности, когда агентства требуют от субъектов сообщать либо рано, либо поздно, в зависимости от серьезности воздействия или значимости затронутой системы.

Анализ информирования о компьютерных инцидентах показывает актуальность проблемы гармонизации подходов в США в рамках решения общей проблемы гармонизации терминологии в сфере компьютерной безопасности.

Дефиниции в сфере защиты информации и информационных технологий

Следует отметить, что в российском понятийном аппарате и нормативной базе соседствуют два понятия: инцидент компьютерной безопасности и инцидент информационной безопасности, которые в разных источниках определяются по-разному. В словаре терминов Банка данных угроз безопасности информации[1] инцидент информационной безопасности определён как «одно или несколько нежелательных или не ожидаемых событий информационной безопасности, которые со значительной вероятностью приводят компрометации бизнес-операций и создают угрозы для информационной безопасности». В национальном стандарте Российской Федерации ГОСТ Р ИСО/МЭК ТО 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности Information technology. Security techniques. Information security incident management» термин «событие информационной безопасности (information security event)» определено как «идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь

[1] См. bdu.fstec.ru

отношение к безопасности (п. 3.2); а «инцидент информационной безопасности (information security incident)» описывается как «появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы ИБ» [п.3.3]. В Положении о мониторинге информации и контроле потенциальных каналов утечки данных в Министерстве Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС России), утвержденном приказом от 20 июля 2022 г. № 725, инцидент информационной безопасности описывается как «появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности информации и создания угрозы утечки информации конфиденциального характера». Сравнение этих терминов показывает, что в каждом из них есть определенные нюансы, отличающие их друг от друга, что подтверждает необходимость гармонизации этого важного термина с учетом международного права и подходов государственных регуляторов.

Существенное расширение доступа к открытой информации, отмечаемое в последнее время, нашло отражение в действующем законодательстве. Международное право и национальное законодательство последних десятилетий показывают значительные изменения в подходе к решению проблемы определения информации ограниченного доступа, проведения правовых разграничений между разными видами информации. Международные правовые акты устанавливают общие основания ограничений. В последние десятилетия отмечается тенденция к определению более конкретных видов информации и документов, доступ к которым ограничен [9, С.76-78].

В статье Артамоновой Г.К., Рыбкиной М.В., Муталиевой Л.С. [10, с.97] изложены итоги участия авторов в практической деятельности по гармонизации законодательств государств-членов Организации Договора о коллективной безопасности (ОДКБ) в рамках рабочей группы, созданной в Санкт-Петербургском университете Государственной противопожарной службы МЧС России. Проведенное ими исследование позволило определить, что гармонизация национальных законодательств в соответствующей области – это приведение национальных нормативных правовых актов в такое соотношение друг с другом, при котором они по своему содержанию, принципам правового регулирования и предполагаемым результатам в правоприменительной практике не противоречат и соотносятся друг с другом.

В качестве одной из проблем, Ю.А. Тихомиров и В.Д. Чураков отмечают необходимость развития ведомственного нормотворчества, потребность в котором особенно ярко проявилась в вопросе приостановления действия устаревших ГОСТов и иных инструкций, разработанных еще в СССР, а также огромного количества различных ведомственных актов, принятых за последние десятилетия. Поток ведомственной регуляции, охватывающей сферы информационной безопасности и защиты информации, постоянно возрастает, что только добавляет проблем. Приостановка в последнее время множества национальных ведомственных регуляторов, содержащих технические регламенты и разные жизненно необходимые для определенной деятельности инструкции и правила, грозит новыми проблемами в технологической, информационной и других сферах. Многие инструкции и рекомендации связаны с международными стандартами, следовательно, их приостановление может привести к нарушению этих стандартов. Поэтому процесс приостановления национальных ведомственных регуляторов вызывает неудовлетворенность [11, с.41-49]. В связи с упорядочиванием ведомственного нормотворчества в контексте «регуляторной гильотины» целесообразно вести работу системно, не сводя ее исключительно к отбору обязательных для государственного управления и бизнеса требований.

По мнению Ю.А. Тихомирова и В.Д. Чуракова

до сих пор остается неясным вопрос, касающихся соотношения и приоритета международных и национальных регуляторов. Следует согласиться с их мнением, что самый очевидный ответ содержится в ст. 15 Конституции РФ. Однако указанная норма сформулирована очень нечетко. Не ясно, кто устанавливает случаи противоречия, предусмотренные ч. 4 ст. 15 Конституции РФ, а также на какой период времени приостанавливается действие национальных регуляторов. Кроме того, отсутствует структурированность международных регуляторов. В рамках ООН, МОТ, СНГ, ЕАЭС действуют разные акты, часто не сходных по содержанию. Процессы суверенизации и глобализации нередко противоречат друг другу, вследствие чего возрастает роль права [11, с.41] в гармонизации этих противоречивых процессов в сфере обеспечения информационной безопасности и защиты информации.

Процесс правообразования, как справедливо писал в 1910-1912 гг. известный русский юрист-правовед Г.Ф. Шершеневич, «испытывает на себе еще действие весьма крупного фактора – заимствования. Право не развивается в недрах одного народа теми силами, какие заложены в данном общественном союзе. Национальный характер право носит только в самом начале культурной жизни, когда общественный союз держится изолированно, как это было с jus civile римлян. Чем больше втягивается народ в жизнь других народов, тем более испытывает он воздействие чужого права» [12, с.121]. Эти суждения юриста особенно актуальны в сфере информатизации и компьютерной безопасности, где много терминов заимствовано из англосаксонского права, что объективно связано с бурным лидирующим развитием средств вычислительной техники и информационных технологий на Западе, начиная с середины 1970-х годов.

Немецкий философ И. Кант указывал, что дать дефиницию – это значит первоначально и полно изложить понятие в его границах, что предполагает ясность и достаточность (одновременно и неизбыточность) признаков, отличающих определенный предмет [13, с.430-433]. При формулировании законодательных дефиниций, по мнению исследователей, необходимо соблюдать определенные правила [14, с.36-43; 15, с.88]:

– определение должно содержать существенные видовые и родовые признаки определяемого термина;

– оно формулируется при помощи слов, выражений и других терминов, значения которых известны или более ясны и понятны, чем значение определяемого термина;

– определяющая часть законодательной дефиниции не может содержать определяемый термин;

– взаимосвязанные термины не могут определяться друг через друга таким образом, что каждый термин, входящий в состав сложного описания, вводится ранее или разъясняется позднее через вводимый термин.

Базовый термин «защита информации» в Федеральном законе от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» в определяющей части содержит определяемый термин. В частности, в статье 16 Закона установлено, что «защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации» [15].

Однако, в Положении о мониторинге информации и контроле потенциальных каналов утечки данных в МЧС России, утвержденным приказом от 20.07.2022 № 725, «защита информации» определяется более широко как «деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информации».

На примере антивирусных мер, которые относятся как к правовым и организационным, так и техническим мерам, можно доказать, что выделение трех групп мер (правовых, организационных и технических) весьма условно и не дает полного представления о содержании защитных мер. Определенные сложности существуют и при отнесении криптографических мер к одной из выше указанных групп. Например, в законодательстве Российской Федерации при определении средств защиты информации выделяют технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации [16].

В нормативных правовых актах, регулирующих правовые отношения в сфере информации, информационных технологий и защиты информации используют два способа определения терминов: обобщенный, указывающий на родовой признак и видовое отличие, и перечневый, когда в определении перечисляются действия и явления, охватываемые данным термином.

Например, в качестве обобщённого определения можно назвать понятие «информационно-телекоммуникационная сеть», которое означает технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Перечневым определением является определение термина «информационная технология», под которым понимают «процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» [17, с.89].

Разработчик проекта ведомственного нормативного правового акта должен внимательно отслеживать наличие в действующих законодательных актах дефиниций-терминов, используемых в проектах руководящих документов для того, чтобы не порождать противоречия и коллизии. К сожалению, на практике это требования соблюдается иногда крайне небрежно.

Законодательство Российской Федерации определяет способы доступа к информации о деятельности государственных органов и органов местного самоуправления (ст. 6 Закона об обеспечении доступа). Установленный перечень является открытым. В частности, допускается, что законы, нормативные правовые акты государственных органов, правовые акты органов местного самоуправления могут устанавливать и другие способы доступа.

Право на информацию признается на уровне международных актов. На европейском континенте и в документах Совета Европы и Европейского Союза во второй половине XX века право на информацию и право на доступ к информации получили определенное распространение. Важное значение имеют рекомендации Комитета Министров Совета Европы от 25 ноября 1981 г. № R81(19) о доступе к информации публичной власти. В соответствии с этим документом, государства обеспечивают каждому человеку, находящемуся в пределах юрисдикции любого государства-члена Совета Европы, право получать по запросу информацию, имеющуюся у государственных органов.

Процесс совершенствования новейших информационных технологий и цифровизация получает отражение в законодательстве, хотя и не всегда адекватно. В современных сложных межгосударственных отношениях правовыми средствами воздействия выступают основные принципы международного права, заключение и исполнение международных договоров и деятельность международных межправительственных организаций. В частности, международно-правовое регулирование в сфере связи исследователями характеризуется отсутствием жестких механизмов и процедур контроля и надзора за исполнением международно-правовых норм. Основным способом урегулирования разногласий и споров являются переговоры [6, с.94].

В научной литературе отмечаются либо поспешные действия и решения, либо существенное отставание законодательства от развития

таких технологий. В связи с этим, по-прежнему существует необходимость разработки и правильного использования понятий правового пространства и обеспечения безопасности информации. В результате существенно расширяется научно-информационная база принятия правовых решений и использования юридических и иных прогнозов, диагностики рисков и правового мониторинга.

Одним из показательных примеров противоречивости, несогласованности подходов к режиму безопасности информационного взаимодействия являются положения п.2.1 Единых стандартов обмена информацией информационных систем с автоматизированной информационно-управляющей системой Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (АИУС РСЧС) и п.4 Положения о системе и порядке информационного обмена в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций (ЧС). Определено, что информационные ресурсы в области защиты населения и территорий от ЧС подразделяются на оперативную и плановую информации. К оперативной информации относятся сведения о прогнозируемых и (или) возникших ЧС природного, техногенного, биолого-социального характера и их последствиях, сведения о силах и средствах РСЧС постоянной готовности, привлекаемых для предупреждения и ликвидации ЧС, а также об их деятельности, направленной на предупреждение и ликвидацию ЧС. К плановой информации относятся сведения об административно-территориальных образованиях, об организациях и их деятельности, необходимые для заблаговременного планирования мероприятий по предупреждению и ликвидации ЧС. В плановую информацию в обязательном порядке включаются данные о численности населения административно-территориальных образований и работников организаций. Ответственными за сбор, обработку и передачу оперативной и плановой информации являются органы повседневного управления РСЧС.

В 2021 г. на заседании Правительственной комиссии по предупреждению и ликвидации ЧС и обеспечению пожарной безопасности (протокол от 23 июня 2021 г. №2) были одобрены «Единые стандарты обмена информацией информационных систем с АИУС РСЧС», в п.2.1 которых установлено, что «организация информационного взаимодействия осуществляется с использованием сертифицированных средств криптографической защиты, а также должны быть выполнены требования нормативных правовых актов Российской Федерации в области защиты информации, не составляющей государственной тайны». В действующем приказе МЧС России от 26 августа 2009 г. № 496 «Об утверждении положения о системе и порядке информационного обмена в рамках единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций» согласно п. 4 установлено противоположное Единым стандартам обмена информацией информационных систем с АИУС РСЧС требование: «При сборе, обработке и обмене информацией обязательным условием является соблюдение требований конфиденциальности и защиты информации в соответствии с законодательством Российской Федерации о государственной тайне». Важно отметить, что положения о системе и порядке информационного обмена в рамках РСЧС утверждены в соответствии полномочиями Министерства согласно Положению о МЧС России, утвержденному Указом Президента Российской Федерации от 11 июля 2004 г. № 868.

Следует подчеркнуть, что информационно-телекоммуникационная инфраструктура РСЧС, составляющая техническую основу информационного обмена, строится путем конвергенции на всех уровнях управления различных телекоммуникационных сред в целях формирования единого информационного пространства, а систему такого информационного обмена образуют:

– субъекты информационного обмена, в роли которых выступают постоянно действующие органы управления РСЧС на федеральном, межрегиональном, региональном, муниципаль-

ном и объектовом уровнях;

– информационно-телекоммуникационная инфраструктура РСЧС;

– совокупность информационных ресурсов в области защиты населения и территорий от чрезвычайных ситуаций.

Важным, с точки зрения гармонизации нормативных правовых актов и руководящих документов МЧС России в интересах защиты информации и обеспечения информационной безопасности, является определение таких базовых понятий как «цифровая информационная инфраструктура МЧС России», «конфиденциальная информация», а также определение содержания отдельных условий, касающихся соблюдения требований конфиденциальности и защиты информации при сборе, обработке и обмене информацией в РСЧС.

Понятие «информационная инфраструктура» является одним из базовых в цифровой трансформации и поэтому оно требует углубленного рассмотрения и понимания. В обстановке цифровизации гармонизация законодательства обретает черты актуального, инновационного направления развития государственных органов. Как, не без оснований, полагает М.А. Пшеничнов, что «законы, ввиду того что творятся человеком, обществом, наполнены многочисленными пороками, им сопутствующими. Разрыв между целью закона (реальной либо мнимой, теоретической или практической) и целью, которой пытаются достичь при его помощи – источник дисгармонии. Наличие дисгармонии законодательства становится основной предпосылкой его гармонизации» [18, с.209].

Важным является выделение роли федеральных органов исполнительной власти в гармонизации законодательства. Изменения в условиях переориентации ряда направлений международной гармонизации позволяют достигать конструктивного обеспечения национальных интересов в межгосударственном (в том числе в рамках Евразийского экономического союза – ЕАЭС, Союзного государства Республики Беларусь и Российской Федерации и др.), внутригосударственном и межведомственном взаимодействии. И.Л. Бачило, формируя рекомендации по созданию единого правового пространства Союзного государства России и Белоруссии, определяет гармонизацию законодательства как комплексную систему «деятельности, включающую выявление наличности правовой базы каждого государства; проведение сравнительного анализа, выявление различий и противоречий, пробелов, оценку актуальности и преимуществ законодательства каждой из сторон, выработку прогноза относительно реализации конкретных форм создания единой или унифицированной правовой системы Союза, организацию работы по каждому объекту законодательства с учетом определенной формы его адекватности включения в единое правовое пространство»[19].

Помимо гармонизации в научной литературе выделяют еще унификацию права, а также способ международно-правовой интеграции путем сближения права. Цель сближения заключается в согласованности, устранении противоречий в правовых системах государств. Гармонизация является одним из средств общегосударственной политики совершенствования нормативной и терминологической базы в сфере обеспечения информационной безопасности. Гармонизация преследует важную цель сохранения традиций законодательства, ориентирована в основном на выявление и фиксацию дисгармонии в законодательстве как в аспекте взаимосвязей его внутренних элементов, так и в контексте сопряжения с иными нормативными правовыми актами. Следовательно, гармонизация законодательства предполагает наличие объективных условий сближения отношений в той или иной сфере – наличие оснований для гармонизации [18, с.209]. Гармонизация нормативной правовой базы представляет собой сложный, многомерный и длящийся процесс. Изменчивы информационные и информационно-коммуникационные технологии (ИКТ-технологии), общественная жизнь и законодательство. Затормозить эти взаимосвязанные процессы не представляется возможным.

В научно-концептуальном ракурсе выделяют

два принципиально разных и несоподчиненных уровня гармонизации законодательства: уровень статической гармонизации (гармонизация содержания) и уровень динамической гармонизации (гармонизация действия законов) [18, с.206-210].

В гармонизации выделяют ее принципы – основополагающие идеи, начала, положения. В.М. Баранов и М.А. Пшеничнов в работе [20, с.71-77] во внутригосударственной сфере гармонизация законодательства выделили такие основные начала, как принципы: целесообразности, пропорциональности; сбалансированности; симметричности, вариативности, универсализации, реализма, рентабельности. Кроме того, исследователями определены специфичные принципы гармонизации законодательства и в международно-правовом аспекте: принцип суверенитета законодательства, принцип добросовестного выполнения международных обязательств, принцип взаимности. С этими принципами в целом можно согласиться и дополнить их принципами законности и прогнозирования развития законодательства (объективности и обоснованности; вариативности, непрерывности, согласованности различных видов прогнозирования).

Приоритет национальной терминологии (недопустимость необоснованного использования иностранной терминологии) означает, что иноязычные термины могут использоваться только при наличии определенных предпосылок [21, с.177]. К сожалению, и в техническом регулирования, и в правовой науке, и в юридических документах рассматриваемое требование соблюдается далеко не всегда. Так, действующее российское законодательство в информационной сфере перегружено заимствованными иностранными терминами (в основном латинского и англоязычного происхождения, например, «инфраструктура» и т.д.). Термин «инфраструктура» исходит от лингвистического содержания латинских слов «infra» (ниже) и «strnctura» (строение, взаиморасположение, что возможно интерпретировать как фундамент). Существуют различные подходы к толкованию этимологии слова. Например, такое представление, что инфраструктура – это комплекс взаимосвязанных обслуживающих структур, составляющих и/или обеспечивающих основу для решения проблемы (задачи).

Информационную инфраструктуру определяют как взаимосвязанную совокупность информационных систем и подсистем. Коммуникационная инфраструктура нередко определяют через понятие сетевой инфраструктуры, обеспечивающей передачу информации между территориально распределенными источниками и получателями, состоящая из линий связи, оборудования, обеспечивающего прием, передачу и обработку электромагнитных сигналов.

Одно из значений термина рассматривается как базовая структура или особенности системы или организации. В разделе 42 Кодекса США § 18445(c) термин «информационная инфраструктура» означает базовую структуру, на которую опираются информационные системы и активы для обработки, передачи, получения или хранения информации в электронном виде, включая программируемые электронные устройства и сети связи, а также любое связанное с ними оборудование, программное обеспечение или данные.

Информационная инфраструктура Российской Федерации, согласно Доктрине информационной безопасности РФ (пп. «з» п. 2), также не содержит антропогенный компонент. Информационная инфраструктура России обеспечивает возможность сбора, передачи, хранения, обработки и распространения информации. Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры РФ является основным национальным интересом в информационной сфере. В п. 28 Стратегии развития информационного общества в РФ на 2017–2030 гг., утвержденной Указом Президента РФ от 9 мая 2017 г. № 203, определено несколько уровней информационной инфраструктуры: программное обеспечение и сервисы, предоставляемые с использованием сети Интернет; информационные системы и центры обработки данных; сети связи (линии и средства

связи, инфраструктура российского сегмента сети Интернет, технологические и выделенные сети связи, сети и оборудование интернета вещей). Пониманию содержания термина «информационная инфраструктура» помогают, определенные в статье 2 Федерального закона от 26.07.2017 г. № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» определения объектов и субъектов критической информационной инфраструктуры. В частности, критическая информационная инфраструктура – это объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. В рассматриваемое понятие субъекты не включены. Следовательно, можно предположить, что «ИТ-инфраструктура» – это совокупность средств реализации процессов, методов поиска, сбора, хранения, обработки, предоставления, нематериальных активов организаций для достижения результата, создания конечного продукта, обеспечивающего функционирование и развитие организации.

Определения, которые охватываются социально-техническим взглядом, описывают находящиеся в постоянном взаимодействии социальные и технические аспекты информационной деятельности.

Трудно спорить с утверждением, что любая отрасль теории и практики базируется на строгом понятийном аппарате. Поэтому важно понять содержание терминов «автоматизированная система» и «информационная система». Современные определения обычно основаны на онтологической позиции, в которой люди и технологии по своей сути разделены. В соответствии с различными интерпретациями понятий могут различаться и подходы к защите информации в рассматриваемых системах. Однако объективные процессы показывают наличие определенного потенциала для разработки альтернативной социально-материальной концепции информационной безопасности. Если рассуждать с позиций формальной логики, отбросив слово «система», мы можем сравнить определения терминов «автоматизированная» и «информационная». Даже поверхностный взгляд показывает их существенные внешние различия. Однако интерес представляет прежде всего их содержательное наполнение. Термин «информационная система» в отечественной и зарубежной литературе трактуется и как техническая система, реализованная с использованием компьютерных и телекоммуникационных технологий, и, в контексте обеспечения информационных потребностей организации, как социальная система, и как концептуальная система, в которой сочетаются вышеперечисленные подходы. Автоматизированные информационные системы (ИС) предполагают участие в процессе обработки информации человека и технических средств. При этом средствам вычислительной техники отводится ключевая роль в выполнении рутинных операций обработки данных, что соответствует современному представлению ИС. Профессор Н.А. Гайдамакин предлагает под ИС понимать организованную «совокупность программно-технических и других вспомогательных средств, технологических процессов и функционально-определенных групп работников, обеспечивающих сбор, представление и накопление информационных ресурсов в определенной предметной области, поиск и выдачу сведений, необходимых для удовлетворения информационных потребностей установленного контингента пользователей - абонентов системы»[22,с.14]. Участие человека предопределяет особенности защиты информации в ИС, так как человек является субъектом доступа и его наличие формирует потенциальные угрозы и находит отражение в модели нарушителя и модели угроз безопасности информации. Мировой опыт реализации компьютерных атак показывает, что нередко они совершаются сотрудниками организации (иногда бывшими) или при их непосредственном участии.

В Федеральном законе РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Закон

№ 149) понятие ИС раскрывается как совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств. В действующем законе сохраняется правовая позиция об исключении человека (персонала) из элементов системы.

Изучение научных публикаций показывает, что термин «информационная система» используется в широком (включая персонал) и в узком (исключая персонал) смысле. Используя герменевтический подход для проведения литературных обзоров, авторами статьи «Что такое Информационная система?» выделено четыре различных взгляда на ИС [23]:

– технологический;

– социальный;

– социально-технический, подчеркивающий взаимосвязь технологий и социальных элементов;

– представление процесса, характеризующее направленность деятельности ИС, а также обоснование необходимости разработки дополнительной, альтернативной социоматериальной концептуализации ИС, основанной на недуалистической, относительной онтологии.

Одно из наиболее широких определений ИС дал М.Р. Когаловский, включив в него системный персонал [24]. Американский исследователь Гордон Б.Дэвис в определение информационной системы также включает персонал, которым используются информационные технологии в целях предоставления информационно-коммуникационных услуг для обработки транзакций (операций) и управления организацией. Системы используют комбинацию автоматизации, действий человека и взаимодействия пользователя и машины [25, с. 67].

С позиций защиты информации и обеспечения безопасности персональных данных при их обработке в ИС рассмотрим предложенное ФСТЭК России толкование соотношения понятий «информационная система» и «автоматизированная система». В Информационном сообщении ведомства от 15 июля 2013 г. № 240/22/2637 в связи с изданием приказов ФСТЭК России от 11 февраля 2013 г. № 17 и от 18 февраля 2013 г. № 21 регулятор сделал сообщение о том, что в нормативных правовых актах ФСТЭК используется понятие «информационная система», установленное Законом № 149. В иных методических документах и национальных стандартах в области защиты информации используется понятие «автоматизированная система», определенное национальным стандартом ГОСТ 59853-2021 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», в котором автоматизированная система (АС) определена как «система, состоящая из комплекса средств автоматизации, реализующая информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование».

Важным для анализа содержания понятия «цифровая информационная инфраструктура» (ЦИИ) МЧС России и, в утратившем актуальность, ГОСТ 34.003-90 является дефиниция «комплекс средств автоматизации автоматизированной системы», которая представлена в качестве «совокупности всех компонентов АС, за исключением людей». Это положение в дальнейшем будет использовано при конструировании авторского понятия ЦИИ МЧС России.

Как уже отмечалось, в понятие ЦИИ МЧС России входят в качестве составляющего элемента автоматизированные системы, которые вносят диссонанс в относительно устоявшееся в России современное понимание информационной инфраструктуры и ее правовое содержание на настоящем историческом этапе развития информационных систем. Для гармонизации термина ЦИИ МЧС России предлагаем, в рамках сложившихся в настоящее время в российском законодательстве и науке доминирующих представлений о понятии «инфраструктура», скорректировать применение в определении ЦИИ МЧС России термина «автоматизированные системы» путем отражения только его части, не связанной с персоналом. В результате исследования предлагается две возможные редакции определения понятия

ЦИИ.

Цифровая информационная инфраструктура – это совокупность государственных информационных систем, информационных систем, комплексов средств автоматизации деятельности персонала (иначе, комплексов средств автоматизации автоматизированной системы), реализующих информационные технологии выполнения установленных функций, информационно-телекоммуникационных сетей, центров обработки данных, телекоммуникационного оборудования, средств защиты информации, средств вычислительной техники и средств отображения информации МЧС России, имеющих подключение к ведомственной цифровой сети связи с интеграцией услуг.

Интеграционные и дезинтеграционные политические, военно-политические, правовые и социально-экономические процессы, способствующие активному созданию региональных сообществ, являются одной из ключевых характеристик современного мира не только на уровне доктрины, но и в практической деятельности по обеспечению информационной безопасности. Очевидно, что это достаточно сложный процесс, предполагающий как политическую, так и правовую интеграцию его участников. Многие авторы указывают на необходимость создания технологий сближения национальных правовых систем в целях обеспечения наиболее эффективного развития региональных и глобальных объединений. Решение этой задачи становится одним из основных направлений развития мировой правовой системы[26].

Еще в своем докладе 3 апреля 2014 г. на VI Международной научно-практической конференции – Кутафинские чтения «Гармонизация российской правовой системы в условиях международной интеграции» академик РАН Т.Я. Хабриева отмечала, что «российская и зарубежная правовая наука уже давно констатирует сближение национальных правовых систем, отмечая процессы правовой гармонизации»[27].

В условиях конфликтного противостояния России с недружественным блоком стран Запада во главе с США в системе российского законодательства и техническом регулировании происходят важные, порой кардинальные по охвату и темпам, реформы и процессы, направленные на совершенствование терминологического аппарата и нормативной правовой базы в сфере информационной безопасности и защиты информации. Одновременно проявления дисгармонии в определении терминов в техническом регулировании и российском законотворчестве выступают следствием несовершенства его организации, порой ошибочности либо явной медлительности нормотворческих и правоприменительных инициатив [26, с.195].

В Стратегии национальной безопасности Российской Федерации [28], утверждённой Указом Президента Российской Федерации от 2 июля 2021 № 400, «информационная безопасность» определена в качестве стратегического национального приоритета после сбережения народа России и развития человеческого потенциала, обороны страны, государственной и общественной безопасности. За счет концентрации усилий и ресурсов органов публичной власти, организаций и институтов гражданского общества на обеспечении информационной безопасности осуществляются обеспечение и защита национальных интересов Российской Федерации.

В определениях информационная безопасность рассматривается и через призму трех защитных свойств информации-конфиденциальности, целостности и доступности, и с добавлением еще четырех дополнительных свойств – недоказуемости, подотчётности, аутентичности и достоверности информации, а также через цели обеспечения информационной безопасности без конкретизации технологий, механизмов, методов и средств их достижения. Приведем ряд таких определений информационной безопасности:

– состояние защищенности информации организации, при котором обеспечиваются конфиденциальность, доступность и целостность;

– защита конфиденциальности, целостности и доступности информации [29];

– все аспекты, связанные с определением,

достижением и поддержанием конфиденциальности, целостности, доступности, недоказуемости, подотчетности, аутентичности и достоверности информации или средств ее обработки [30,31];

– защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации;

– защищенность информационных активов организации. Уровень защищенности определяется либо требованиями правовых норм к информационным активам, либо возможностями самой организации и степени понимания необходимости защиты владельцем информационных активов [5, с.28].

Отсутствие четкого правового регулирования процесса гармонизации в сфере обеспечения информационной безопасности усиливает значимость научно-исследовательских разработок в рассматриваемой сфере, в связи с чем, вопросы гармонизации обеспечения безопасности ведомственной информации выдвигаются на первый план. Их важная роль заключается в создании правовых условий развития органов государства, которым постоянно приходится сталкиваться с увеличением и обострением внешних и внутренних вызовов, кризисных ситуаций.

В отношении обеспечения безопасности информации практика показала важность и целесообразность осуществления процесса гармонизации национальных законодательств и межведомственной гармонизации. Достоинствами этого процесса можно назвать следующие: выработка единообразных подходов в правовом регулировании вопросов (например, межведомственного информационного взаимодействия); наиболее эффективная реализация прав и свобод граждан, участвующих в гармонизации; эффективность механизма межведомственного сотрудничества органов государства в сфере обеспечения безопасности информации. Гармонизация законодательства, регулирующего различные аспекты обеспечения информационной безопасности, является в настоящее время актуальной задачей и отражает объективную необходимость в рамках межведомственного взаимодействия при ликвидации чрезвычайных и иных кризисных ситуаций.

В частности, основными принципами в сфере гармонизации национальных законодательств государств являются:

– приоритетность общепризнанных норм и принципов международного права над актами национального законодательства;

– взаимное уважение государственного суверенитета;

– уважение прав и свобод человека и гражданина;

– принцип равенства участников процесса гармонизации;

– согласованность правового регулирования;

– принцип единого информационно-правового пространства государств-участников процесса гармонизации;

– интеграция национальных правовых систем в соответствующей области, подлежащей гармонизации;

– взаимодействие с иностранными государствами, межгосударственными и иными организациями в соответствующей области, подлежащей гармонизации [10, с.97].

Теоретически можно выделить следующие этапы гармонизации нормативных правовых актов в обеспечении безопасности информации:

– определение основных принципов, целей и задач гармонизации в обеспечении безопасности информации;

– анализ состояния правовой базы федеральных органов исполнительной власти и МЧС России, выявление различий, противоречий, пробелов, включая оценку актуальности и преимуществ законодательства каждого министерства и ведомства;

– определение соответствия нормативной правовой базы МЧС России общепризнанным нормам и принципам правового регулирования;

– осуществление конкретных юридических действий по приведению подзаконных актов МЧС России в соответствие с требованиями государственных регуляторов положениями международ-

ных соглашений и общепризнанными нормами и принципами международного права в обеспечении безопасности информации соответствующей области;

– использование гармонизированных актов в деятельности в федеральных органах исполнительной власти в обеспечении безопасности информации МЧС России, государств и международных организаций;

– оценка достигнутых результатов на межведомственном и внутриведомственном уровнях;

– определение направлений и содержания последующих этапов внутриведомственной гармонизации нормативной правовой базы в сфере обеспечения информационной безопасности и защиты информации.

В теории осуществление гармонизации связывают со следующими уровнями гармонизации:

– гармонизация на межгосударственном уровне;

– «вертикальная», иерархическая гармонизация национального законодательства, включая ведомственную нормативную правовую базу;

– «горизонтальная» гармонизация, например, на уровне нормативных правовых актов МЧС России и правовых актов территориальных органов и организаций МЧС России;

– гармонизация на уровне правовой нормы в пределах отдельного правового акта МЧС России.

Е.Е. Орлова наиболее очевидными формами сближения правового регулирования выделяет:

– синхронизация права (все варианты политико-правовой координации между интегрирующимися правовыми системами);

– гармонизация права (сложное, разноуровневое явление, состоящее из двух стадий: гармонизации законодательства и гармонизации правового регулирования, соотносящиеся между собой как часть и целое);

– унификация права (имплементация, принятие одинаковых нормативных правовых актов не только по содержанию, но и по форме) [26, с.10].

Учеными-юристами акцентируется внимание на возросшую после распада СССР конкуренцию правовых сообществ и семей. Мониторинг законодательства показывает, что правовая система России испытывает влияние как родственной ей семьи континентального или романо-германского права, так и семьи общего права. В отечественную правовую систему все чаще проникают не только отдельные институты, но и фундаментальные начала общего права. Например, англосаксонская концепция верховенства права все чаще подменяет континентальную идею правового государства, обоснованную в трудах В.Д. Зорькина [32]. И все большее число государств следуют в русле общего права, придавая прецедентную силу судебным решениям.

Академик Т.Я. Хабриева, подчеркивая все большую скорость развития процессов сближения правовых институтов, выделяет следующие особенности развития процессов правовой гармонизации:

– процессы в этой области развиваются по-разному, в разных формах и с разной степенью сближения национальных правовых систем. Как показывает практика, высокая степень правовой гармонизации возможна в основном в рамках однородных правовых сообществ и семей. Гармонизация правовых систем государств, различающихся по своей социально-экономической сущности (например, Франции и Китая), может осуществляться только в ограниченных пределах;

– процессы правовой гармонизации государств разной социально-экономической сущности требуют времени;

– различаются алгоритмы гармонизации разных правовых институтов [27].

Заключение

1. В целях развития доктрины информационного права, в части обеспечения информационной безопасности, разработано понятие процесса гармонизации законодательства об информации, информационных технологиях и о защите информации, которое представляет собой нормотворческий процесс, направленный на сближение и устранение различий в терминологических системах законодательной базы Российской Федерации и государств-членов

международных интеграционных объединений для создания условий эффективного функционирования развития международного сотрудничества в сфере обеспечения информационной безопасности, в том числе, включающий совместную деятельность государств-членов в проведении единой политики в обеспечении безопасности информации и углубления цифровой трансформации.

2. Ведомственному правовому регулированию в сфере обеспечения безопасности информации не хватает системности. Система правового регулирования по обеспечению информационной безопасности и защиты информации становится в современный период более сложной и динамичной. Кроме национально-правовых в нее включаются международно-правовые регуляторы. Соотношение этих регуляторов нередко бывает неустойчивым и противоречивым. Развитие ведомственной подсистемы должно полностью соответствовать требованиям законодательства Российской Федерации и учитывать основные внутригосударственные и международные позитивные тенденции.

3. Масштабность правового регулирования в рамках МЧС России предполагает выявление разных векторов использования статусов. Осуществление общей политики безопасности, обеспечивающей интеграцию информационных ресурсов при взаимодействии АИУС РСЧС с внешними взаимодействующими информационными системами – источниками и потребителями информации.

На первом этапе гармонизации ведомственной нормативной правовой базы в сфере обеспечения информационной безопасности и защиты информации на первый план выдвигаются задачи создания условий успешной правовой гармонизации:

– инвентаризация действующих документов МЧС России и разработка ведомственного нормативного правового акте, систематизирующего ключевые направления интеграции в соответствии законодательством Российской Федерации об информации, информационных технологиях и о защите информации, основанном на Конституции Российской Федерации, международных договорах Российской Федерации;

– преодоление существующей рассогласованности и противоречивости правовой базы действующих ведомственных правовых документов в сфере обеспечения информационной безопасности и защиты информации, гармонизация нормативной правовой базы в сфере защиты сведений конфиденциального характера;

– решение проблемы множественности правовых подходов к определению защищаемой информации в МЧС России;

– взаимная корреляция и определение приоритетности наслаивающихся международных обязательств;

– подготовка и принятие единого нормативного правового акта в МЧС России, инкорпорирующего правовые решения базовых интеграционных соглашений с целью создания единого ведомственного информационного пространства на основе уточнения правового понятия «цифровая информационная инфраструктура МЧС России»;

– модернизация и адаптация постановлений Правительства Российской Федерации и иных межведомственных соглашений, регулирующих различные аспекты обеспечения информационной безопасности при создании и эксплуатации информационных систем единоговедомственного информационного пространства;

– систематизация и актуализация внутриведомственных решений в сфере обеспечения информационной безопасности.

4. Проведенный анализ содержания понятия «информационная система» в сравнении с понятием «автоматизированная система» показывает их определенные различия. Выделенные различия вступают в противоречие с подходом к защите информации как комплексу взаимосвязанных и взаимозависимых правовых, организационных, технических и иных мер, который должен основываться на четких представлениях о системных элементах и о всей системе, как объекте защиты от актуальных угроз безопасности. Для дальнейшего развития сферы обеспечения информаци-

онной безопасности в МЧС России необходима разработка непротиворечивого термина «цифровая информационная инфраструктура МЧС России», которая позволила бы установить единую терминологию, единую цель, единые принципы и единый путь движения Министерства в условиях цифровой экономики.

5. Анализ ведомственного правопонимания природы конфиденциальной информации, ее признаков, а также возможность выделения самостоятельных видов конфиденциальной информации с целью изучения особенностей отношений, возникающих в связи с ее использованием и защитой в МЧС России, показывает необходимость выработки рекомендации по гармонизации правовой базы для решения проблем, связанных с правовым регулированием конфиденциальной информации и служебной информации ограниченного распространения в МЧС России.

Список литературы

1. *Пшеничнов М.А.* Гармонизация российского законодательства (теория, практика, техника). Автореф.тдис.... д-ра юридич. наук: 12.00.01/ Пшеничнов Михаил Александрович.–Нижний Новгород, 2011. – 58 с. – EDN ZOOXCB.

2. *Тихомиров Ю.А.* Коллизионное право. – М.: Российская государственная библиотека, 2000. – 394 с. – EDN QQKPMP.

3. *Камалова Г.Г.* Правовое обеспечение конфиденциальности информации в условиях развития информационного общества: автореферат диссертации на соискание ученой степени доктора юридических наук: 12.00.13 / Камалова ГульфияГафиятовна .– Москва, 2020. – 52 с. – EDN NMDFKG.

4. Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации»// Собрание законодательства Российской Федерации. –2021. – № 27 (часть II). –Ст. 5351.

5. *Минзов А.С.* Методология применения терминов и определений в сфере информационной, экономической и комплексной безопасности бизнеса: уч.-мет. пособие /А.С. Минзов; под ред. Л.М.Кунбутаева. – М.:ВНИИгеосистем, 2011. – 83 с. – ISBN 978-5-8481-0083-9. – EDN QUZGFH.

6. Модернизация государственного регулирования деятельности в области связи: научно-практическое пособие/А.А. Ефремов, Ф.А. Лещенков, К.А. Мефодьева [и др.]; отв. Ред. Л.К. Терещенко. –М.:ИНФРА-М,2020. –152с.– ISBN 978-5-16-016076-4. – DOI 10.12737/1080398. – EDN LBVQRQ.

7. *Рассказов Л.П.* Теория государства и права: углубленный курс: учебник. –М.: РИОР: ИНФРА-М, 2015. –559 с.– ISBN 978-5-369-01369-4. – EDN TXAZLV.

8. *Капустин А.Я.* К вопросу о международно-правовой концепции угроз международной информационной безопасности//Журнал зарубежного законодательства и сравнительного правоведения. – 2017. – №6.–С.45-46.– DOI 10.12737/article_5a1e71d7026536.36788152. – EDN YNMBWZ.

9. Право на доступ к информации. Доступ к открытой информации/отв. Ред. И.Ю.Богдановская. – М.:ЗАО «Юстицинформ»,2009. –344с.

10. *Артамонова Г.К., Рыбкина М.В., Муталиева Л.С. Артамонова Г.К., Рыбкина М.В., Муталиева Л.С., Иванов К.М.* Гармонизация законодательств государств как способ сближения норм права, регулирующих схожие общественные отношения // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». – 2016. – №3. – С. 96-101.– EDN XBVWCP.

11. *Тихомиров Ю. А., Чураков В. Д.* Правовые регуляторы в экономике: национальное и международное измерение // Законодательство. – 2019. – № 8. –С. 41-49.– EDN TVKYVN.

12. *Шершеневич Г.Ф.* Общая теория права: Учебное пособие. В 2-х томах.Т.2. Вып.2,3,4. – М.:Изд-во «Юридический колледж МГУ»,1995. –362с.

13. *Кант И.* Критика чистого разума. –М.,1994. – С.430-433.

14. *Чиннова М.В.* Правила формулирования легального определения// Право и политика. –2005. –№1. –С.36-43.

15. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»(ред. от 12 декабря 2023) //Собрание законодательства Российской Федерации. –2006. –№31 (часть I) . – Ст. 3448.

16. Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне» (ред. от 4 августа 2023)//Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. –1993. – № 38. – Ст. 1480.

17. *Васильева Т.А.* Как писать закон/ Т.А. Васильева. – М.: Издательство Юрайт, 2012. –148 с.

18. *Пшеничнов М.А.* Гармонизация законодательства как объект инновационных научных исследований (к методологии анализа). Юридическая наука и практика//Экономическая безопасность России: политические ориентиры, законодательные приоритеты, практика обеспечения: Вестник Нижегородской академии МВД России. – 2009. – № 2. – С. 206-210. – EDN LANCRB.

19. *Якунин В.И.* Проблемы международной гармонизации железнодорожного права России: монография/ В.И. Якунин; Центр проблемного анализа и гос.-упр. проектирования. – М.: Науч. эксперт, 2008. – 238 с. – ISBN 978-5-91290-037-2. – EDN RAYFQR.

20. *Баранов В.М., Пшеничнов М.А.* Гармонизация законодательства как базовая юридическая конструкция инновационного правового развития государства // Юридическая техника. – 2013. – № 7-2. – С. 71-77. – EDN RBRRQL.

21. Юридическая техника: учебник / под ред. В. М. Баранова. – Москва: Проспект, 2021. – 648 с.

22. *Гайдамакин Н.А.* Автоматизированные информационные системы, базы и банки данных. Вводныйкурс: учебноепособие. –М.: ГелиосАРВ, 2002. – 368 с.

23. *Boell S. K., Cecez-Kecmanovic D.* What is an information system? // 2015 48th Hawaii International Conference on System Sciences. – IEEE, 2015. – P. 4959-4968. – DOI: https://doi.org/10.1109/HICSS.2015.587

24. *Когаловский М.Р.* Перспективные технологии информационных систем. –М.: ДМК Пресс. –288 с. – EDN TLVZWV.

25. *Davis G. B.* Information systems conceptual foundations: looking backward and forward // Organizational and Social Perspectives on Information Technology: IFIP TC8 WG8. 2 International Working Conference on the Social and Organizational Perspective on Research and Practice in Information Technology June 9–11, 2000, Aalborg, Denmark. – Boston, MA : Springer US, 2000. – P. 61-82. – DOI: https://doi.org/10.1007/978-0-387-35505-4_33

26. *Орлова Е.Е.* Гармонизация правового регулирования занятости населения государств-участников СНГ в контексте евразийской перспективы:монография / Е. Е. Орлова. – Тамбов: Издательский центр ФГБОУ ВО «ТГТУ», 2021. – 252 с.

27. Хабриева Т.Я. Гармонизация правовой системы РФ в условиях международной интеграции: вызовы современности// Журнал зарубежного законодательства и сравнительного правоведения. – 2014. – № 1(44). – С. 4-15. – EDN SDIGFJ.

28. Указ Президента РФ от 2 июля 2021 г. N 400 «О Стратегии национальной безопасности Российской Федерации»// Собрание законодательства Российской Федерации от 5 июля 2021 г. № 27 (часть II) ст. 5351.

29. Стандарт ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

30. Стандарт ГОСТ Р ИСО/МЭК 13335-1-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных технологий».

31. Стандарт ГОСТ Р ИСО/МЭК 13335-3-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий».

32. Доктрины правового государства и верховенства права в современном мире / под ред. В.Д. Зорькина, П.Д. Баренбойма. – М., 2013. –

560 с. – EDN YHOACX.

References

1. *Pshenichnov M.A.* Harmonization of Russian legislation (theory, practice, technology).Abstract of dis.... Doctor of Law: 12.00.01 / Pshenichnov Mikhail Aleksandrovich.- Nizhny Novgorod, 2011. – 58 p.– EDN ZOOXCB.

2. *TikhomirovYu.A.*Conflict of laws.- M .: Russian State Library, 2000. - 394 p. - EDN QQKPMP.

3. *Kamalova G.G.* Legal support for the confidentiality of information in the context of the development of the information society: abstract of the dissertation for the degree of Doctor of Law: 12.00.13 / KamalovaGulfiyaGafiyatovna.- Moscow, 2020. - 52 p.- EDN NMDFKG.

4. Decree of the President of the Russian Federation of July 2, 2021 No. 400 "On the National Security Strategy of the Russian Federation" // Collection of Legislation of the Russian Federation.-2021. - No. 27 (Part II).- Art.5351.

5. *Minzov A.S.* Methodology for the Application of Terms and Definitions in the Sphere of Information, Economic and Integrated Business Security: teaching aid / A.S.Minzov;edited by L.M. Kunbutaev.- Moscow: VNIIGeosistem, 2011.– 83 p.– ISBN 978-5-8481-0083-9.- EDN QUZGFH.

6. Modernization of State Regulation of Activities in the Field of Communications: a Scientific and Practical Handbook / A.A.Efremov, F.A. Leshchenkov, K.A.Mefodieva [et al.];Ed.OK.Tereshchenko.– M.: INFRA-M, 2020.–152s.– ISBN 978-5-16-016076-4.– DOI 10.12737/1080398.– EDN LBVQRQ.

7. *Rasskazov L.P.* Theory of state and law: advanced course: textbook.–M.: RIOR:INFRA-M, 2015.– 559 p.– ISBN 978-5-369-01369-4.– EDN TXAZLV.

8. *Kapustin A.Ya.* On the International Legal Concept of Threats to International Information Security // Journal of Foreign Legislation and Comparative Law.- 2017. – No. 6. – P. 45-46.– DOI 10.12737/article_5a1e71d7026536.36788152.– EDN YNMBWZ.

9. The Right to Access to Information.Access to Public Information / Ed.I.Yu.Bogdanovskaya.- M .: ZAO "Yustitsinform", 2009. - 344 p.

10. *Artamonova G.K., Rybkina M.V., Mutalieva L.S. Artamonova G.K., Rybkina M.V., Mutalieva L.S., Ivanov K.M.* Harmonization of state legislations as a way of bringing together legal norms regulating similar social relations // Scientific and analytical journal "Bulletin of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia".- 2016. - No. 3. - P. 96-101.- EDN XBVWCP.

11. *Tikhomirov Yu.A., Churakov V.D.* Legal regulators in the economy: national and international dimension // Legislation.- 2019. - No. 8. - P. 41-49.- EDN TVKYVN.

12. *Shershenevich G.F.* General Theory of Law: A Textbook.In 2 volumes.V. 2. Issues 2,3,4.- M .: Publishing house "Law College of Moscow State University", 1995. - 362 p.

13. *Kant I.* Critique of Pure Reason.– M., 1994. – P.430-433.

14. *Chinnova M.V.* Rules for formulating a legal definition // Law and Politics.– 2005. – No. 1. –P.36-43.

15. Federal Law of July 27, 2006 No. 149-FZ "On Information, Information Technologies and Information Protection" (as amended on December 12, 2023) // Collection of Legislation of the Russian Federation.- 2006. - No. 31 (Part I) .- Art.3448.

16. Law of the Russian Federation of July 21, 1993 No. 5485-I "On State Secrets" (as amended on August 4, 2023) // Bulletin of the Congress of People's Deputies of the Russian Federation and the Supreme Council of the Russian Federation.- 1993. - No. 38. - Art.1480.

17. *Vasilyeva T.A.*How to write a law / T.A.Vasilyeva.- M .: Yurait Publishing House, 2012. -148 p.

18. *Pshenichnov M.A.* Harmonization of legislation as an object of innovative scientific research (towards the methodology of analysis).Legal science and practice // Economic security of Russia: political guidelines, legislative priorities, practice of provision: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia.– 2009. – No. 2. – P. 206–210.– EDN LANCRB.

19. *Yakunin V.I.* Problems of international harmonization of railway law of Russia: monograph / V.I. Yakunin;Center for problem analysis and state-

management design.- M .: Scientific expert, 2008. – 238 p.- ISBN 978-5-91290-037-2. –EDN RAYFQR.

20. *Baranov V.M., Pshenichnov M.A.* Harmonization of legislation as a basic legal structure of innovative legal development of the state // Legal technique.– 2013. – No. 7-2.– pp. 71-77.– EDN RBRRQL.

21. Legal technique: textbook / edited by V. M. Baranov.- Moscow: Prospect, 2021. - 648 p.

22. *Gaidamakin N.A.* Automated information systems, databases and data banks.Introductory course: tutorial.- M .: Gelios ARV, 2002. - 368 p.

23. *Boell S.K., Cecez-Kecmanovic D.* What is an information system?// 2015 48th Hawaii International Conference on System Sciences.- IEEE, 2015. - P. 4959-4968.- DOI: https://doi.org/10.1109/HICSS.2015.587

24. *Kogalovsky M.R.* Promising technologies of information systems.-M .: DMK Press.-288 p.– EDN TLVZWV.

25. *Davis G.B.* Information systems conceptual foundations: looking backward and forward // Organizational and Social Perspectives on Information Technology: IFIP TC8 WG8.2 International Working Conference on the Social and Organizational Perspective on Research and Practice in Information Technology June 9–11, 2000, Aalborg, Denmark.– Boston, MA : Springer US, 2000. – P. 61-82.– DOI: https://doi.org/10.1007/978-0-387-35505-4_33

26. *Orlova E.E.* Harmonization of legal regulation of employment of the population of the CIS member states in the context of the Eurasian perspective: monograph / E. E. Orlova.– Tambov: Publishing center of FGBOU VO "TSTU", 2021. – 252 p.

27. *KhabrievaT.Ya.* Harmonization of the legal system of the Russian Federation in the context of international integration: challenges of our time // Journal of Foreign Legislation and Comparative Law.- 2014. - No. 1 (44).- P. 4-15.- EDN SDIGFJ.

28. Decree of the President of the Russian Federation of July 2, 2021 N 400 "On the National Security Strategy of the Russian Federation" // Collection of Legislation of the Russian Federation of July 5, 2021 N 27 (Part II) Art.5351.

29. Standard GOST R ISO / IEC 17799-2005 "Information technology. Practical rules for information security management".

30. Standard GOST R ISO / IEC 13335-1-2006 "Information technology. Security methods and tools. Part 1. Information technology security management concept and models".

31. Standard GOST R ISO / IEC 13335-3-2006 "Information technology. Security methods and tools. Part 3. Information technology security management methods".

32. Doctrines of the rule of law and the rule of law in the modern world / edited by V.D.Zorkin, P.D.Barenboim.– M., 2013. – 560 p.– EDN YHOACX.

Статья подготовлена в рамках выполнения в 2024 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России, НИР «Разработка принципов, методологии и элементов технологии решения прикладных задач гармонизации нормативной правовой базы в части требований информационной и кибербезопасности в интересах МЧС России» («Гармония»).

Статья поступила в редакцию 16 апреля 2024 г.
Принята к публикации 20 июня 2024 г.

Ссылка для цитирования: Метельков А.Н., Александрова А.Ю. Отечественный и мировой опыт гармонизации нормативных правовых актов в сфере обеспечения безопасности информации // Национальная безопасность и стратегическое планирование. 2024. № 2(46). С. 42-65. DOI: https://doi.org/10.37468/2307-1400-2024-2-42-65

For citation: Metelkov A.N., Alexandrova A.Yu. Domestic and international experience in harmonizing regulatory legal acts in the field of information security // National security and strategic planning. 2024. № 2(46). pp. 42-65. DOI: https://doi.org/10.37468/2307-1400-2024-2-42-65

Сведения об авторах:

МЕТЕЛЬКОВ АЛЕКСАНДР НИКОЛАЕВИЧ – *кандидат юридических наук, доцент кафедры прикладной математики и информационных технологий, Санкт-Петербургский университет Государственной противопожарной службы МЧС России имени Героя Российской Федерации генерала армии Е.Н. Зиничева, г. Санкт-Петербург, Россия*
ORCID: https://orcid.org/0000-0002-5194-7021
SPIN-код: 5990-6833
e-mail: metelkov5178@mail.ru

АЛЕКСАНДРОВА АЛЕНА ЮРЬЕВНА – *старший преподаватель кафедры гражданского права, Санкт-Петербургский университет Государственной противопожарной службы МЧС России имени Героя Российской Федерации генерала армии Е.Н. Зиничева, г. Санкт-Петербург, Россия*
ORCID: https://orcid.org/0000-0002-6113-8981
SPIN-код: 8061-4302
e-mail: alena.karpacheva@inbox.ru

Information about authors:

METELKOV ALEXANDER N. – *Candidate in LawScience, Associate Professor, Department of Applied Mathematics and Information Technology, St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia named after Hero of the Russian Federation, Army General E.N.Zinichev, St. Petersburg,Russia*
ORCID: https://orcid.org/0000-0002-6113-8981
SPIN-код: 5990-6833
e-mail: metelkov5178@mail.ru

ALEXANDROVA ALENAYU. – *Senior Lecturer, Department of Civil Law, St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia named after Hero of the Russian Federation, Army General E.N. Zinichev, St. Petersburg, Russian Federation*
ORCID: https://orcid.org/0000-0002-5194-7021
SPIN: 8061-4302
e-mail: alena.karpacheva@inbox.ru