Научная статья
УДК 004.056; DOI: 10.61260/2218-13X-2025-2-77-90

ФОРМИРОВАНИЕ МЕТОДОЛОГИИ ГАРМОНИЗАЦИИ НОРМАТИВНОЙ ПРАВОВОЙ БАЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ МЧС РОССИИ

✉**Буйневич Михаил Викторович.**
Санкт-Петербургский университет ГПС МЧС России, Санкт-Петербург, Россия
✉***bmv1958@yandex.ru***

Аннотация. Работа посвящена решению задачи гармонизации нормативной правовой базы информационной безопасности и защиты информации для МЧС России, для чего потребовалось формирование соответствующей методологии. Показаны основные противоречия предметной области в нотации категориального анализа, а именно между: устареванием и обновлением нормативной правовой базы информационной безопасности и защиты информации; количеством и качеством нормативных правовых документов; глобальными/национальными и ведомственными/государственными интересами в инфосфере. Выдвинута гипотеза, что все выявленные противоречия не являются антагонистическими, и, следовательно, смягчение их последствий может быть предметом гармонизации.

Синтезированы принципы гармонизации, которые могут выступать как (принципиальные) требования к методологии и специальной информационной технологии решения прикладных задач гармонизации нормативной правовой базы информационной безопасности и защиты информации: научной обоснованности в смысле системности, логичности, необходимости и достаточности, формализуемости, однозначности и достоверности; реализуемости в смысле детерминированности, результативности и массовости, а также наличия инструментария; расширяемости в смысле пула прикладных задач и методов их решения; прагматичности в смысле базиса для выработки научно-обоснованных предложений и рекомендаций по гармонизации.

Установлено, что методология, адекватная решению такой масштабной и трудноформализуемой задачи, как гармонизация нормативной правовой базы информационной безопасности и защиты информации, в настоящий момент отсутствует (или неизвестна). Дано понятие гармонизации нормативной правовой базы информационной безопасности и защиты информации в широком и узком смысле слова. Для последней определены цели: первичная – сопоставимость, вторичная – установление эквивалентности по форме/содержанию и идентичности. Приведена формальная запись собственно идеи такой гармонизации и ее вторичных целей; первичная понимается через онтологию предметной области и достигается единством сущностного алфавита разметки нормативных правовых документов. Предложена методологическая схема гармонизации нормативной правовой базы информационной безопасности и защиты информации в виде логической взаимоувязанной (по исходным данным и результатам) последовательности этапов. Приведен пример работоспособности предлагаемой методологии и определен пополняемый пул прикладных задач гармонизации нормативной правовой базы информационной безопасности и защиты информации для МЧС России.

Сделаны выводы относительно новизны и практической значимости полученных результатов, а также направления дальнейших исследований.

Ключевые слова: информационная безопасность и защита информации, нормативная правовая база, принципы гармонизации, методология гармонизации, прикладные задачи, специальная технология решения

Для цитирования: Буйневич М.В. Формирование методологии гармонизации нормативной правовой базы информационной безопасности и защиты информации для МЧС России // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2025. № 2. С. 77–90. DOI: 10.61260/2218-13X-2025-2-77-90.

Scientific article

DESIGN OF METHODOLOGY FOR REGULATORY LEGAL FRAMEWORK ON INFORMATION SECURITY AND PROTECTION HARMONIZATION FOR EMERCOM OF RUSSIA

✉**Buinevich Mikhail V.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***bmv1958@yandex.ru***

Abstract. The work is devoted to solving the problem of harmonizing the regulatory legal framework on Information Security and Protection for EMERCOM of Russia, which required creating an appropriate methodology. The main contradictions of subject area in the categorical analysis notation are shown, namely between: obsolescence and updating of the regulatory legal framework on Information Security and Protection; normative legal documents quantity and quality; global/national and departmental/state interests in the infosphere. It is hypothesized that all the identified contradictions are not antagonistic and, therefore, their mitigation can be subject of harmonization.

The harmonization principles have been synthesized, which can act as (principled) requirements to methodology and special information technology for solving applied harmonization tasks of the regulatory legal framework on Information Security and Protection. First, scientific validity principle, in the sense of systematicity, logicality, necessity and sufficiency, formalisability, unambiguity and reliability. Secondly, realisability principle, in the sense of determinacy, effectiveness and massiveness, as well as the tools availability. Thirdly, extensibility principle, in the sense of the applied problems pool and methods of their solution. Fourthly, pragmatism principle, in the sense of a basis for developing evidence-based proposals and recommendations for harmonization.

It has been found that there is no (or no known) methodology suitable for solving such a large and difficult to formalize task as harmonizing of the regulatory legal framework on Information Security and Protection. The harmonization notion of the regulatory legal framework is defined in a broad and narrow sense. For the latter, the objectives are defined: primary – comparability, secondary – establishment of equivalence in form/content and identity. A formalized record of such harmonization idea and its secondary aims is given; primary is understood through the ontology of subject area and is achieved by the essence alphabet unity of normative legal documents markup. A methodological scheme for harmonization of the regulatory legal framework on Information Security and Protection is proposed in the form of a logically linked (by initial data and results) stages sequence. An example of proposed methodology workability is given and a replenishable pool of the regulatory legal framework on Information Security and Protection harmonization applied tasks for EMERCOM of Russia is defined.

Conclusions are drawn regarding the novelty and practical significance of the results obtained, as well as directions for further research.

Keywords: information security and protection, regulatory legal framework, harmonization principles, harmonization methodology, applied tasks, special solution technology

For citation: Buinevich M.V. Design of methodology for regulatory legal framework on information security and protection harmonization for EMERCOM of Russia // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2025. № 2. P. 77–90. DOI: 10.61260/2218-13X-2025-2-77-90.

Введение

Специалистам в области информационной безопасности и защиты информации (ИБиЗИ), заинтересованным субъектам сегодня невозможно обойтись без знания и исполнения требований соответствующей нормативной правовой базы (НПБ).

Проведенный автором категориальный анализ современного состояния и тенденций развития НПБ ИБиЗИ позволил выявить ее следующие основные противоречия [1].

Во-первых, с одной стороны, область ИБиЗИ является очень динамичной, что требует постоянного обновления ее НПБ; с другой стороны, руководящие документы де-юре должны содержать сведения, полученные де-факто и накопленные годами в процессе «Best Practices». Налицо объективное противоречие между устареванием vs обновлением НПБ обеспечения деятельности в сфере ИБиЗИ.

Во-вторых, с одной стороны, область ИБиЗИ является достаточно обширной, что предполагает значительный объем знаний для ее освоения; с другой стороны, руководящие документы де-юре должны содержать сведения, полученные де-факто и накопленные годами в процессе «Best Practices»? Налицо противоречие между количеством vs качеством «единиц документных текстов» НПБ обеспечения деятельности в сфере ИБиЗИ.

В-третьих, с одной стороны, область ИБиЗИ является транснациональной, что предполагает учет общемировых тенденций; с другой стороны, вся нормотворческая деятельность должна осуществляться не в ущерб информационному суверенитету Российской Федерации. Налицо противоречие между глобальными и национальными интересами в инфосфере, которое находит свое отражение в нормативно-правовой плоскости, что отмечено, например, в источнике [2].

Традиционно гармонизация понимается как приведение в соответствие отечественного законодательства с мировым (так называемая «внешняя», межгосударственная гармонизация); в международно-правовой сфере гармонизация находится среди основных форм сотрудничества государств. Однако в свете последних политических событий и ретроспективно осознавая ошибочность «слепого копирования», в частности для ИБ, зарубежных стандартов в 1990–2000 гг., это направление остается важным только для взаимодействия с дружественными или нейтральными странами.

В-четвертых, с одной стороны, в бурное развитие отрасли ИБиЗИ неизбежно вовлечено и МЧС России со своей спецификой, которая находит отражение, в том числе, в соответствующих ведомственных Руководящих документах (РД), с другой стороны, все субъекты ИБиЗИ должны строго выполнять требования Регуляторов в этой сфере деятельности и разрабатывать свои РД в согласованности с их НПБ (так называемая «внутренняя», внутригосударственная гармонизация). Налицо противоречие между ведомственными и государственными интересами в инфосфере.

Задача усложняется отсутствием гармонизированной терминологической базы, без которой невозможно ни международное, ни какое-либо другое сотрудничество и взаимодействие (не говоря уже о том, что требования формулируются в терминах сферы применения). Формированию гармонизированной терминологической базы системы обеспечения информационной безопасности МЧС России, в частности, была посвящена плановая научно-исследовательская работа (НИР) шифр «Модель», выполненная по госзаданию в Санкт-Петербургском университете ГПС МЧС России в 2023 г.

Все перечисленные противоречия не являются антагонистическими (либо – либо), и, следовательно, смягчение их последствий может быть предметом гармонизации.

Очевидно, что с учетом этих причин совершенствование нормативного правового (информационного) обеспечения деятельности в сфере ИБиЗИ конфиденциального характера в МЧС России является насущной проблемой, разрешение которой лежит в плоскости гармонизации НПБ, и, в частности, разработки методологии (далее – Методология) и специальной информационной технологии (далее – Технология) решения прикладных задач.

Принципы гармонизации НПБ ИБиЗИ

Результаты анализа подходов к решению проблемы гармонизированных регуляторных изменений в смежных предметных областях, проведенного Санкт-Петербургским университетом ГПС МЧС России в рамках НИР «Гармония» (госзаказ), а также авторский опыт в решении частных задач гармонизации требований позволили сформулировать следующие принципы (П_N, где N – условно-порядковый номер принципа П) гармонизации НПБ ИБиЗИ, которые могут выступать как (принципиальные) требования к Методологии и специальной информационной Технологии решения прикладных задач гармонизации. Ниже приведены эти принципы и их смысловая нагрузка.

Во-первых, принцип *научной обоснованности* (П_1) в смысле *системности* (П_1.1), *логичности* (П_1.2), *необходимости и достаточности* (П_1.3), *формализуемости* (П_1.4), *однозначности* (П_ 1.5) и *достоверности* (П_1.6).

Системность (**П_1.1**) предполагает учет всех взаимодействующих, взаимосвязанных и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения задачи гармонизации, и достигается их описанием в рамках (нотации) единой модели предметной области.

Логичность (**П_1.2**) обеспечивается последовательностью и непротиворечивостью описания предметной области в соответствии с законами логики (в частности, причинно-следственной связи между элементами используемой модели предметной области).

Необходимость и достаточность (**П_1.3**): первая доказывается востребованностью источника знаний (например, основания классификации или сравнения признаков) для решения задачи гармонизации, а вторая – отсутствием корреляции или ортогональностью в соответствующем пространстве (измерении) выбранных признаков гармоничности.

Формализуемость (**П_1.4**) – представление предметной области и решаемых в ней задач в виде символических моделей, позволяющих проводить исследование условий их решения с использованием математических методов.

Однозначность (**П_1.5**) – недвусмысленность, единственность. В контексте задачи гармонизации предполагает наличие терминологического консенсуса. Требование более чем актуальное по причине существующей вариативности определений в сфере ИБ-понятий и отсутствия устоявшейся (и тем самым – «негостированной») терминологии в сфере кибербезопасности.

Достоверность (**П_1.6**) – обоснованность, доказательность, истинность. Как правило, обеспечивается корректностью постановки решаемой научной задачи, строго обоснованной совокупностью ограничений и допущений, представительным библиографическим материалом, опорой на современную научную базу, корректным применением апробированных классических и современных методов; подтверждается непротиворечивостью полученных результатов передовым практикам (Best Practices), а также апробацией результатов на представительных научных форумах и публикацией в рецензируемых научных изданиях.

Во-вторых, принцип *реализуемости* (П_2) в смысле *детерминированности* (П_2.1), *результативности* (П_2.2) и *массовости* (П_2.3), а также *наличия инструментария* (П_2.4).

Детерминированность (**П_2.1**) – признак (требование) технологичности, когда каждое действие (операция, указание, шаг, требование), направленное на получение конечного продукта, понимается в строго определённом (однозначном) смысле, исключающем произвольное толкование (трактование).

Результативность (**П_2.2**) – признак (требование) технологичности, при котором процесс выполнения последовательности детерминированных действий должен приводить к определённому ожидаемому (гарантируемому при соблюдении технологической дисциплины) результату.

Массовость (**П_2.3**) – признак (требование) технологичности, при котором гарантируется неоднократность получения ожидаемого результата, а также тиражируемость самой технологии.

Наличие инструментария (**П_2.4**) предполагает либо наличие конкретных средств решения задачи, либо возможность выбора и обоснование такого средства, либо реалистичную возможность его разработки в допустимое время.

В-третьих, принцип *расширяемости* (П_3) в смысле пула прикладных задач (П_3.1) и методов их решения (П_3.2). Расширяемость предполагает, что как пул прикладных задач гармонизации, так и пул соответствующих методов их решения не является окончательным и может быть дополнен новыми элементами по мере надобности и с развитием научно-методической базы.

И в-четвертых, принцип *прагматичности* (П_4) в смысле базиса для выработки научно-обоснованных предложений и рекомендаций по гармонизации. Предполагается, что и Методология и специальная информационная Технология решения прикладных задач гармонизации призваны содействовать этой выработке.

Далее по тексту эти принципы (вернее, их условно-порядковые номера) будут контекстно расставлены.

Формирование методологии гармонизации НПБ ИБиЗИ для МЧС России

Как установлено в п. 1.5 отчета о НИР «Гармония» (это показал аналитический обзор отечественного и мирового опыта гармонизации), Методология, адекватная решению такой масштабной и трудноформализуемой задачи, как гармонизация НПБ ИБиЗИ (Гармонизация), в настоящий момент отсутствует (или неизвестна).

Значит вопрос о том «с использованием приложенных к каким данным каких методов, взаимоувязанных в логическую последовательность, возможно решение задачи Гармонизации?» является проблемным и открытым.

Так как выбор и обоснование состава методов зависит от особенностей процесса получения желаемого результата, целесообразно его сформулировать. Но прежде следует разделить понятие Гармонизации в широком и узком смысле слова, как имеющие разные цели.

Гармонизация НПБ в широком смысле (Гармонизация_1) понимается как безколлизионное и полное «покрытие» онтологической (связе-сущностной) модели предметной области нормативно-правовыми документами. Для демонстрации работоспособности этого определения примем за такую модель «ландшафт» информационной безопасности, представленный на рисунке.

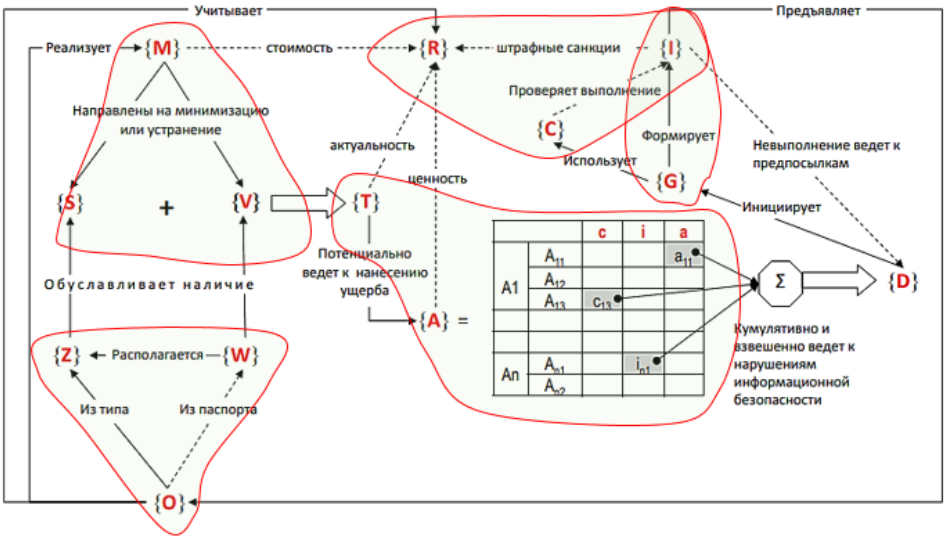

Рис. **«Ландшафт» информационной безопасности**

На рисунке приняты следующие условные обозначения сущностей информационной безопасности: {**O**} – операторы (*от англ.* **O**perator); {**W**} – оборудование (**W**are); {**Z**} – зоны

(**Z**one) безопасности; {**V**} – уязвимости (**V**ulnerability);{**S**} – источники (**S**ource) угроз; {**T**} – угрозы (**T**hreat); {**A**} – активы (**A**sset); {**c**} – ущерб конфиденциальности (**c**onfidentiality) актива;{**i**} – ущерб целостности (**i**ntegrity) актива; {**a**} – ущерб доступности (**a**vailability) актива; {**D**} – нарушения (**D**amage); {**G**} – регуляторы (**G**overnment); {**I**} – требования (**I**nsistence) к оператору; {**M**} – защитные меры (**M**easure); {**R**} – методы и средства оценки рисков (**R**isk); {**C**} – методы и средства проверки выполнения (**C**hecking) требований (по ИБиЗИ).

С позиций системного и причинно-следственного анализа автором в работе [3] изложен методологический подход (**П_1.1**), связывающий требования к оператору (в части требований информационной безопасности) с нарушениями конфиденциальности, целостности и доступности информации, суть которого состоит в следующем:

– государством (в лице регулятора) к оператору (O, Operator) предъявляются требования (I, Insistence), которые реализуются им в виде защитных мер и мероприятий (M, Measures), направленных на минимизацию или устранение источников угроз (S, Source) и уязвимостей (V, Vulnerability), обусловленных наличным операторским оборудованием (W, Ware) и зоной его расположения (Z, Zone);

– оператор определяет состав защитных мер и мероприятий, исходя из баланса их стоимости, ценности защищаемых активов, штрафных санкций за невыполнение требований и актуальности угроз, определяемых с помощью методов и средств оценки рисков {R, Risk};

– выполнение требований, предъявляемых к оператору, проверяется с помощью соответствующих методов и средств (C, Checking);

– источник угроз (при наличии соответствующей уязвимости) потенциально ведет к реализации угроз (T, Threat), создающих опасность нанесения ущерба конфиденциальности (c, confidentiality), целостности (i, integrity) и доступности (a, availability) активов (A, Assets) оператора, который, в свою очередь, кумулятивно и взвешенно ведет к нарушениям (D, Damage) информационной безопасности.

Таким образом, по установленной причинно-следственной цепочке (**П_1.2**), невыполнение оператором предъявляемых ему требований ведет к предпосылкам соответствующих нарушений (рис.).

Как видно из рисунка, во-первых, отсутствует полное «покрытие» онтологической модели предметной области ИБиЗИ – сущность «D» оказалась «непокрытой» НПБ, а во-вторых, присутствует коллизия – сущность «I» оказалась «покрытой» более чем одним элементом из множества НПБ. То есть для данного примера цели Гармонизации_1 не достигнуты.

Гармонизация НПБ в рамках НИР «Гармония» понималась в узком смысле (Гармонизация_2) как приведение в соответствие НПБ ведомства в области ИБиЗИ к НПБ Регуляторов.

При всем кажущемся разнообразии понятия «приведение в соответствие» применительно к двум нормативным правовым документам (НПД[1]), множество целей Гармонизации_2 в конченом счете сводится к приведенным в табл. 1.

Таблица 1

Цели Гармонизации_2

По форме	По содержанию	Цель (степень) Гармонизации_2
+	+	идентичность
+	–	эквивалентность по форме
–	+	эквивалентность по содержанию
–?	–?	сопоставимость

[1] Дословно – нормативный правовой документ; по факту – документ, подлежащий гармонизации: нормативный правовой акт, правовой акт, руководящий документ

Их необходимость и достаточность (**П_1.3**) гарантируется применением естественной для данной задачи категориальной пары «форма vs содержание». Применимость этой пары для задач ИБиЗИ многократно доказана в работах Буйневича М.В. и Израилова К.Е. [4–8]. В частности, аналитическое моделирование работы программного кода с уязвимостями и схема жизненного цикла программы позволили дать научно-обоснованные определения цели (степени) Гармонизации_2 и ввести элементы их формализации.

Под идентичностью понимается полное совпадение двух НПД и по форме, и по содержанию. Под эквивалентностью – тождественность (максимально близкое соответствие) двух НПД либо по форме, либо по содержанию. Под сопоставимостью понимается обеспечение сравнимости двух НПД.

Достижение (установление, определение) идентичности и эквивалентности возможно только после достижения сопоставимости двух НПД. Тогда первые три цели Гармонизации_2 могут квалифицироваться как вторичные по отношению к первичной цели – сопоставимости.

Формальная запись (**П_1.4**) собственно идеи Гармонизации_2 и ее вторичных целей приведена ниже.

Очевидно, что в каждый документ заложена некоторая суть, понимаемая его создателем (автором, разработчиком) – N_i (*от англ*. Notion). Тогда сам документ – P_i (Paper) будет обладать некоторой внешней формой – F_i (Form) и внутренним содержанием – C_i (Content), которые были получены из его исходной сути некоторыми действиями (как правило, имеющими творческую природу):

$$N_i \equiv \langle F_i, C_i \rangle.$$

Так, любая идея при передаче другому субъекту может быть записана в виде документа на разговорном языке (то есть иметь текстовую форму) и обладать определенными законами изложения (то есть иметь логику содержания). При этом как форма, так и содержание должны основываться на некотором базисе – B_i (Basis), на элементах которого они построены – B_i^F и B_i^C (например, синтаксис языка и онтология). Таким образом, получение формы и содержания документа из его сути может быть записано следующим образом:

$$\begin{cases} F_i = Creation^F(S_i, B_i^F) \\ C_i = Creation^C\left(S_i, B_i^C\right), \end{cases}$$

где $Creation^{\cdots}(\ldots)$ – оператор создания формы и содержания, что указано в его верхнем индексе.

Тогда полная гармонизация (идентичность) двух документов (i и j) означает соответствие базисов их формы и содержания, то есть:

$$\begin{cases} B_i^F = B_j^F \\ B_i^C = B_j^C. \end{cases}$$

В ином случае даже документы будут отличаться по форме и/или содержанию:

$$\forall i, j, i \neq j: \left(B_i^F \neq B_j^F \bigvee B_i^C \neq B_j^C\right) \Rightarrow P_i \neq P_j.$$

Частичная гармонизация (эквивалентность) соответствует неполному выполнению условий (первое уравнение – гармонизация только по форме, второе – только по содержанию):

$$\begin{bmatrix} B_i^F = B_j^F \wedge B_i^C \neq B_j^C \\ B_i^C \neq B_j^C \wedge B_i^C = B_j^C. \end{bmatrix}$$

Соответственно, полное отсутствие гармонизации двух документов может быть записано следующим образом:

$$\begin{cases} B_i^F \neq B_j^F \\ B_i^C \neq B_j^C. \end{cases}$$

Первичная цель Гармонизации_1 – сопоставимость – определяется возможностью сравнения сути НПД, которая понимается через онтологию предметной области и достигается единством сущностного алфавита их разметки.

Для решения декларированного выше проблемного вопроса предлагается следующая методологическая схема Гармонизации_2 в виде логической взаимоувязанной (по исходным данным и результатам) последовательности этапов m (m = 1, M) достижения цели: (исходные данные)$_1$ → (назначение и метод обработки)$_1$ → (результат)$_1$ = (исходные данные)$_2$ → (назначение и метод обработки)$_2$ → (результат)$_2$ = … (исходные данные)$_m$ → (назначение и метод обработки)$_m$ → (результат)$_m$ = … (исходные данные)$_M$ → (назначение и метод обработки)$_M$ → (результат)$_M$.

Для удобства восприятия этапы Гармонизации_2 и их содержание представлено в табличном виде (табл. 2).

Таблица 2

Содержание этапов Гармонизации_2

Этап	Исходные данные	Назначение обработки	Метод	Результат
1	Предметная область	Получение алфавита для разметки	Онтологическое моделирование	Сущности и сущностные связи предметной области (алфавит разметки)
2	НПД + алфавит разметки	Разметка пула НПД	Анкетирование по шаблону	Пул размеченных НПД
3	> 1 размеченного НПД	Сопоставление	Посущностное сравнение	Первичная степень гармонизации
4	> 1 сопоставленного НПД	Эквивалентность по форме/содержанию	Формальное сравнение / сравнение терминологических базисов (**П_1.5**)	Вторичная степень гармонизации
5	Идентичность НПД в контексте цели и задач НИР не рассматривалась			

Перейдем от методов к способам поэтапного решения задачи, которые предполагают уже наличие формы и инструментария.

Все методы исполняются экспертами (то есть вручную) (**П_2.4**), но различной квалификации (высшей – на Этапе_1 и Этапе_3, средней – на Этапе_2).

Возможна передача миссии автомату (программе) по мере углубления формализации задачи или по мере развития технологии искусственного интеллекта (в частности – машинного обучения) (**П_2.4**) [9].

Этап_1. В качестве инструментальной онтологической модели предлагается представленный выше «ландшафт» (рис.).

Этап_2. В качестве шаблона используется специально разработанная электронная анкета табличного вида «сущность × структурный элемент документа», где последний может быть указан как абзац, глава (параграф), раздел (подраздел), пункт (подпункт), приложение, рисунок, статья, страница. Для повышения достоверности полученных результатов (**П_1.6**) вместо технически затрудненного увеличения количества раундов оценки[2] применено анкетирование в двух группах по два эксперта в каждой.

Условный пример результатов экспертного опроса (фрагмент анкеты) по использованию сущностей «ландшафта» в руководящих и нормативных документах МЧС России (представленных на Гармонизацию_2) и Регуляторов ИБиЗИ приведен в табл. 3.

Таблица 3

Пример заполненной анкеты

Сущность	Название документа: **Концепция информационной безопасности МЧС России (утверждена решением коллегии МЧС России от 4 июня 2019 г. № 4/I) [11]**
	группа №
{A}	подр. 2.2, п. 2.2.1, 2.2.2
{C}	п. 8.4.3, подр. 9.2, 9.3
{D}	
{G}	подр. 1.2, 1.3, п. 6.2.5, 8.2.2, Прил. 12
{I}	подр. 1.4, 4.2, п. 6.1.1, 6.1.2, 6.2.1–6.2.4, 6.2.6, 6.3.1, 7.1.2, 7.2.1–7.2.7, 8.1.1–8.1.4, подр. 8.2, 8.3, п. 8.4.2, подр. 9.1, Прил. 6, 8, 10
{M}	подр. 4.3, п. 6.2.1, 6.2.5, 6.3.1–6.3.3, Прил. 1 рис. 4, Прил. 2 разд. 2, Прил. 5, Прил. 9
{O}	подр. 3.1–3.7
{R}	подр. 1.5, 5.4, п. 7.2.7, Прил. 4, Прил. 12
{S}	п. 5.2.1
{T}	п. 5.1.1–5.1.3, Прил. 1 рис. 2, Прил. 3, 4
{V}	Прил. 3
{W}	подр. 2.3
{Z}	подр. 1.6, п. 7.2.3, Прил. 11
{c}	подр. 5.3
{i}	подр. 5.3
{a}	
A→R	
C→I	подр. 9.2, 9.3
D→G	
G→C	
G→I	подр. 4.2
I→D	
I→O	подр. 1.1
I→R	
M→R	Прил. 5
M→S	п. 6.2.1, Прил. 9
M→V	Прил. 9
O→M	подр. 4.3

[2] В методике оценки угроз безопасности информации (утв. ФСТЭК России 5 февр. 2021 г.) [10] рекомендуется не менее двух

Сущность	Название документа: **Концепция информационной безопасности МЧС России (утверждена решением коллегии МЧС России от 4 июня 2019 г. № 4/I) [11]**
O→R	
O→W	подр. 2.3
O→Z	подр. 3.1–3.5
S+V→T	
T→A	п. 5.1.2, Прил. 3, 4
T→R	п. 5.1.3, Прил. 3, 4
W→V	
W→Z	
Z→S	
(a)→D	
(c)→D	подр. 5.3
(i)→D	подр. 5.3

Сокращения: разд. – раздел НПД, подр. – подраздел, п. – пункт, Прил. – приложение, рис. – рисунок.

Если отдельные результаты экспертного опроса в обеих группах не совпали, то добавляется раунд оценки или коллизию разрешает «старший» эксперт.

Этап_3. На этом этапе размеченные НПД (Регуляторов и ведомственные) сравниваются экспертами посущностно; по результатам сравнения (НПД гармонизированы только по форме и/или содержанию или негармонизированы) формулируются предложения по внесению изменений в НПД (**П_4**).

Сопоставление НПД по форме/содержанию (вторичная степень гармонизации) может быть затруднено ввиду значительного содержательного объема сущностей «ландшафта». В этом случае сущность должна быть декомпозирована на подсущности требуемой (для решения прикладных задач гармонизации) глубины стратификации, и уже этими подсущностями будут размечены НПД.

Покажем это на примере сущности «Требования» («I»), которая может быть декомпозирована на требования к:

1) функциональной организационной структуре (составу и содержанию подсистем);

2) подсистемам СОИБ[3], например, обнаружения вторжений;

3) функциональным элементам СОИБ, средствам защиты информации (ЗИ) (например, межсетевому экрану);

4) организации защиты информации;

5) мерам защиты информации;

6) субъектам СОИБ;

7) жизненному циклу СОИБ или информационных систем в защищенном исполнении и др.

Такая возможность (в смысле детального сравнения по конкретному требованию, например, к длине пароля или к организации учета машинных носителей) заложена в предлагаемую Методологию (за счет вариабельности и стратифицируемости сущностного алфавита разметки – замены/модификации и/или масштабирования «Ландшафта») и может быть реализована в рамках Специальной информационной технологии (**П_2.1** – **П_2.4**).

В практической плоскости разработанная Методология находит свое отражение в решении прикладных задач (ПЗ) гармонизации НПБ ИБиЗИ для МЧС России, которые могут быть представлены в виде следующего пополняемого (**П_3.1**) пула (задач):

ПЗ_1. Добавление НПД в информационное хранилище;

ПЗ_2. Разметка НПД (требуемой глубины);

ПЗ_3. Хранение НПД в выбранном формате;

ПЗ_4. Актуализация информационного хранилища (обновление состава и содержания НПД);

ПЗ_5. Поиск НПД по ключевым словам (сущностям);

[3] СОИБ – система обеспечения информационной безопасности [11].

ПЗ_6. Сопоставление (сравнение) > 1 НПД по ключевым словам (сущностям);

ПЗ_7. Содержательный анализ НПД;

ПЗ_8. Выработка и обоснование рекомендаций по гармонизации НПБ.

Практическая реализация стратифицированного подхода гармонизации требований наталкивается на отсутствие не только утвержденных (общепринятых, регламентированных, гостированных) классификаций требований ИБиЗИ, но и научных публикаций в открытом доступе по ключевым словам «классификация требований» (в контексте ИБиЗИ).

Существующие же перечни требований от Регуляторов также не могут претендовать на их классификацию по причине переменного («блуждающего») основания. Так, в Руководящих и методических документах Федеральной службы по техническому и экспортному контролю [12, 13] перечисляются «Требования к мерам защиты информации, содержащейся в информационной системе», которые должны обеспечивать:

– идентификацию и аутентификацию субъектов и объектов доступа (основание классификации = процедура доступа; далее основание классификации – по умолчанию);

– управление доступом субъектов к объектам доступа (механизм защиты);

– ограничение программной среды (механизм защиты);

– защиту машинных носителей информации (объект защиты);

– регистрацию событий безопасности (механизм защиты);

– антивирусную защиту (источник угрозы);

– обнаружение (предотвращение) вторжений (механизм защиты);

– контроль (анализ) защищенности информации (механизм защиты);

– целостность информационной системы и информации (цель ЗИ);

– доступность информации (цель ЗИ);

– защиту среды виртуализации (объект защиты);

– защиту технических средств (объект защиты);

– защиту информационной системы, ее средств, систем связи и передачи данных (объект защиты).

Создание необходимого и достаточного (для решения прикладных задач гармонизации) классификатора требований ИБиЗИ является наукоемкой и сложной задачей, решение которой выходит за рамки настоящей статьи.

Заключение

Выполненная автором работа относится к отчетным материалам НИР «Разработка принципов, методологии и элементов технологии решения прикладных задач гармонизации нормативной правовой базы в части требований информационной и кибербезопасности в интересах МЧС России» (шифр «Гармония», рег. № 123030100009-7), а именно к подразделам 2.1 «Синтез принципов гармонизации нормативной правовой базы информационной безопасности и защиты информации для МЧС России» и 2.2 «Формирование методологии гармонизации нормативной правовой базы информационной безопасности и защиты информации для МЧС России».

Первым научным результатом, изложенным в статье, являются принципы гармонизации НПБ ИБиЗИ, которые образуют стройную систему, где один принцип ассоциирован с другим через проблемные вопросы гармонизации, а более «мелкие» выводятся из содержания «более крупных». Его научная новизна состоит в том, что такая система принципов, нормативно и юридически инвариантная к предметной области своего приложения и одновременно чувствительная к последней – ИБиЗИ, сформулирована впервые.

Теоретическая значимость системы состоит в углублении представлений о принципах гармонизации НПБ, раскрывая и конкретизируя их общее понятие (форму) и содержание, что обеспечивает прояснение условий возможности понимания НПД (герменевтическая функция).

Практическая значимость принципов заключается в том, что они выступают неким критерием истинности знаний, получаемых в процессе исследования предметной области (гносеологическая функция), а также выступают как (принципиальные) требования к Методологии и Специальной информационной технологии решения прикладных задач гармонизации НПБ ИБиЗИ.

В реализации принципов сформирована методология гармонизации НПБ ИБиЗИ для МЧС России – второй научный результат, изложенный в статье. Подобная Методология также получена впервые.

Теоретическая значимость Методологии состоит в формализации как собственно идеи Гармонизации НПБ, так и ее целей и задач в базисе формы и содержания НПД.

Практическая значимость Методологии определяется ее прагматическим характером, что позволяет перейти непосредственно к разработке Специальной технологии решения прикладных задач.

Практическая значимость исследования состоит в возможности использования его результатов при разработке проектов законодательных и иных нормативных правовых актов, а также в судебной и иной правоприменительной практике при толковании действующего законодательства.

Дальнейшие исследования в этом направлении видятся на путях интеграции и активного использования Best Practices, обработанных с помощью методов искусственного интеллекта.

Список источников

1. Буйневич М.В., Примакин А.И. Категориальный анализ проблем гармонизации нормативно-правовой базы информационной безопасности // Информационная безопасность регионов России (ИБРР-2015). 2015. С. 34–35.

2. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности: Указ Президента Рос. Федерации от 12 апр. 2021 г. № 213. Доступ из справ.-правового портала «Гарант».

3. Организационно-техническое обеспечение устойчивости функционирования и безопасности сети связи общего пользования / М.В. Буйневич [и др.]; под. общ. ред. С.М. Доценко. СПб.: Изд-во СПбГУТ, 2013. 142 с.

4. Израилов К.Е., Татарникова И.М. Подход к анализу безопасности программного кода с позиции его формы и содержания // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2019): сб. науч. статей VIII Междунар. науч.-техн. и науч.-метод. конф. СПб, 2019. С. 462–467.

5. Израилов К.Е. Моделирование программы с уязвимостями с позиции эволюции ее представлений. Часть 1. Схема жизненного цикла // Труды учебных заведений связи. 2023. Т. 9. № 1. С. 75–93. DOI: 10.31854/1813-324X-2023-9-1-75-93.

6. Израилов К.Е. Моделирование программы с уязвимостями с позиции эволюции ее представлений. Часть 2. Аналитическая модель и эксперимент // Труды учебных заведений связи. 2023. Т. 9. № 2. С. 95–111. DOI: 10.31854/1813-324X-2023-9-2-95-111.

7. Буйневич М.В., Израилов К.Е. Аналитическое моделирование работы программного кода с уязвимостями // Вопросы кибербезопасности. 2020. № 3 (37). С. 2–12. DOI: 10.21681/2311-3456-2020-03-02-12.

8. Modeling the Development of Energy Network Software, Taking into Account the Detection and Elimination of Vulnerabilities / I. Kotenko [et al.] // Energies. 2023. Vol. 16. Iss. 13. P. 5111. DOI: 10.3390/en16135111.

9. Буйневич М.В. Методы искусственного интеллекта в решении задачи гармонизации нормативно-правового обеспечения пожарной и информационной безопасности для интегрированных систем защиты информации // Пожарная безопасность: современные вызовы. Проблемы и пути решения: материалы Всерос. науч.-практ. конф. СПб, 2024. С. 29–34.

10. Методика оценки угроз безопасности информации: метод. документ (утв. ФСТЭК России 5 февр. 2021 г.). Доступ из справ.-правового портала «Гарант».

11. Концепция информационной безопасности МЧС России (утв. решением коллегии МЧС России от 4 июня 2019 г. № 4/I). Доступ из справ.-правового портала «Гарант».

12. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февр. 2013 г. № 17. Доступ из справ.-правового портала «Гарант».

13. Меры защиты информации в государственных информационных системах: метод. документ (утв. ФСТЭК России 11 февр. 2014 г.). Доступ из справ.-правового портала «Гарант».

References

1. Bujnevich M.V., Primakin A.I. Kategorial'nyj analiz problem garmonizacii normativno-pravovoj bazy informacionnoj bezopasnosti // Informacionnaya bezopasnost' regionov Rossii (IBRR-2015). 2015. S. 34–35.

2. Ob utverzhdenii Osnov gosudarstvennoj politiki Rossijskoj Federacii v oblasti mezhdunarodnoj informacionnoj bezopasnosti: Ukaz Prezidenta Ros. Federacii ot 12 apr. 2021 g. № 213. Dostup iz sprav.-pravovogo portala «Garant».

3. Organizacionno-tekhnicheskoe obespechenie ustojchivosti funkcionirovaniya i bezopasnosti seti svyazi obshchego pol'zovaniya / M.V. Bujnevich [i dr.]; pod. obshch. red. S.M. Docenko. SPb.: Izd-vo SPbGUT, 2013. 142 s.

4. Izrailov K.E., Tatarnikova I.M. Podhod k analizu bezopasnosti programmnogo koda s pozicii ego formy i soderzhaniya // Aktual'nye problemy infotelekommunikacij v nauke i obrazovanii (APINO-2019): sb. nauch. statej VIII Mezhdunar. nauch.-tekhn. i nauch.-metod. konf. SPb, 2019. S. 462–467.

5. Izrailov K.E. Modelirovanie programmy s uyazvimostyami s pozicii evolyucii ee predstavlenij. Chast' 1. Skhema zhiznennogo cikla // Trudy uchebnyh zavedenij svyazi. 2023. T. 9. № 1. S. 75–93. DOI: 10.31854/1813-324X-2023-9-1-75-93.

6. Izrailov K.E. Modelirovanie programmy s uyazvimostyami s pozicii evolyucii ee predstavlenij. Chast' 2. Analiticheskaya model' i eksperiment // Trudy uchebnyh zavedenij svyazi. 2023. T. 9. № 2. S. 95–111. DOI: 10.31854/1813-324X-2023-9-2-95-111.

7. Bujnevich M.V., Izrailov K.E. Analiticheskoe modelirovanie raboty programmnogo koda s uyazvimostyami // Voprosy kiberbezopasnosti. 2020. № 3 (37). S. 2–12. DOI: 10.21681/2311-3456-2020-03-02-12.

8. Modeling the Development of Energy Network Software, Taking into Account the Detection and Elimination of Vulnerabilities / I. Kotenko [et al.] // Energies. 2023. Vol. 16. Iss. 13. P. 5111. DOI: 10.3390/en16135111.

9. Bujnevich M.V. Metody iskusstvennogo intellekta v reshenii zadachi garmonizacii normativno-pravovogo obespecheniya pozharnoj i informacionnoj bezopasnosti dlya integrirovannyh sistem zashchity informacii // Pozharnaya bezopasnost': sovremennye vyzovy. Problemy i puti resheniya: materialy Vseros. nauch.-prakt. konf. SPb, 2024. S. 29–34.

10. Metodika ocenki ugroz bezopasnosti informacii: metod. dokument (utv. FSTEK Rossii 5 fevr. 2021 g.). Dostup iz sprav.-pravovogo portala «Garant».

11. Koncepciya informacionnoj bezopasnosti MChS Rossii (utv. resheniem kollegii MCHS Rossii ot 4 iyunya 2019 g. № 4/I). Dostup iz sprav.-pravovogo portala «Garant».

12. Ob utverzhdenii trebovanij o zashchite informacii, ne sostavlyayushchej gosudarstvennuyu tajnu, soderzhashchejsya v gosudarstvennyh informacionnyh sistemah: prikaz FSTEK Rossii ot 11 fevr. 2013 g. № 17. Dostup iz sprav.-pravovogo portala «Garant».

13. Mery zashchity informacii v gosudarstvennyh informacionnyh sistemah: metod. dokument (utv. FSTEK Rossii 11 fevr. 2014 g.). Dostup iz sprav.-pravovogo portala «Garant».

Информация о статье:
Статья поступила в редакцию: 26.02.2025; одобрена после рецензирования: 22.04.2025;
принята к публикации: 26.04.2025

The information about article:
The article was submitted to the editorial office: 26.02.2025; approved after review: 22.04.2025;
accepted for publication: 26.04.2025

Информация об авторах:
Буйневич Михаил Викторович, профессор кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета ГПС МЧС России (196105, Санкт-Петербург, Московский пр., д. 149), доктор технических наук, профессор, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022, SPIN-код: 9339-3750

Information about authors:
Buinevich Mikhail V., professor department of applied mathematics and information technology security of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovsky ave., 149), doctor of technical sciences, professor, e-mail: bmv1958@yandex.ru, https://orcid.org/0000-0001-8146-0022, SPIN: 9339-3750