УДК 342.7

ГОСУДАРСТВЕННО-ПРАВОВОЙ МЕХАНИЗМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ: СОСТОЯНИЕ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ

Т. Н. Кузьменкова
старший преподаватель
Могилевский государственный университет имени А. А. Кулешова
аспирант
Белорусский государственный университет

Статья посвящена анализу государственных мер противодействия угрозам, возникающим при взаимодействии личности с информационной средой, вектору их оптимизации в контексте функционирования целостного государственно-правового механизма обеспечения информационной безопасности личности. В ходе исследования сформулировано понятие и определена структура предлагаемого механизма, отражены основные направления совершенствования национального законодательства.

Ключевые слова: государственно-правовой механизм, информационная безопасность личности, кибербезопасность, национальная безопасность, права человека, правовой статус личности.

Введение

Развитие общества сопровождается появлением новых сфер, нуждающихся в правовом регулировании. Формирование наиболее оптимальных моделей такого регулирования долгий процесс, на который оказывает влияние множество факторов. Нельзя не согласиться с С. Г. Дробязко, что регулирование не может осуществляться в произвольном порядке. «Регулировать – значит упорядочивать в соответствии с объективно обусловленными потребностями» [1, с. 442]. С учетом тотальной информатизации общества на современном этапе одной из таких сфер выступает защита личности от угроз и вызовов в информационном пространстве. Она требует именно государственно-правовой регламентации, что вытекает из конституционной обязанности власти создавать гарантии реализации прав и свобод человека, а также необходимости отражения интересов государства в области производства, хранения и распространения информации в рамках обеспечения национальной безопасности.

Цель настоящего исследования – проанализировать принимаемые меры, направленные на обеспечение информационной безопасности личности, наметить вектор их развития в контексте функционирования целостного государственно-правового механизма.

Основная часть

Характер существующих угроз личности в информационном пространстве предопределяет существующие средства и методы защиты от их воздействия, ключевую роль среди которых играет государственно-правовое регулирование. Основополагающее значение имеют стратегические документы: Конституция Республики Беларусь; Концепция национальной безопасности Республики Беларусь, Концепция информационной безопасности Республики Беларусь, Концепция обеспечения суверенитета Республики Беларусь в сфере цифрового развития до 2030 года.

11 июля 2025 года вступила в силу Директива Президента Республики Беларусь от 9 апреля 2025 г. № 12 «О реализации основ идеологии белорусского государства», которой сформирована конкретная ценностно-мировоззренческая модель, именуемая идейной основой, состоящая из культурно-исторического, политического, экономического и социального компонентов, пронизывающих все сферы государственной и общественной жизни, в том числе область обращения информации. Применительно к сфере обеспечения информационной безопасности личности в аспекте фильтрации подаваемого контента Директива №12 предписывает субъектам реализации идеологии белорусского государства обеспечить «оценку художественной продукции, рекламы, информационного, публицистического и развлекательного контента на предмет соответствия основам идеологии белорусского государства» [2].

Более предметное регулирование обеспечения безопасности личности при ее взаимодействии с информационной средой содержится в нормативных правовых актах, непосредственно затрагивающих вопросы обращения информации: Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», Закон Республики Беларусь от 17 июля 2008 г. № 427-З «О средствах массовой информации», Закон Республики Беларусь 7 мая 2021г. №99-З «О защите персональных данных», Закон Республики Беларусь от 10 мая 2007 г. № 225-З «О рекламе», Положение о порядке и сроках реагирования на общественно значимую информацию, утвержденное Постановлением Совета Министров Республики Беларусь 30 декабря 2024 г. № 1039 и других актах законодательства. Ответственность за нарушение законодательства, направленного на обеспечение информационной безопасности личности, отражена в нормах Уголовного Кодекса Республики Беларусь и Кодекса Республики Беларусь об административных правонарушениях путем закрепления соответствующих составов правонарушений.

В целях реализации принятых в государстве норм созданы институциональные гарантии – совокупность соответствующих органов, учреждений, организаций, в том числе Оперативно-аналитический центр при Президенте Республики Беларусь (далее ОАЦ), аттестованные центры кибербезопасности, Национальный центр защиты персональных данных Республики Беларусь, Министерство связи и информатизации Республики Беларусь, Министерство информации Республики Беларусь.

Вместе с тем несмотря на принятые в государстве меры, направленные на обеспечение информационной безопасности, отсутствует общая стратегия обеспечения именно безопасности личности в информационном пространстве, эти вопросы во многом урегулированы фрагментарно. «В настоящее время четко не определено, какой государственный орган и каким образом реализует функции государственного регулирования в области обеспечения информационной безопасности личности [3, с. 27].

Подобное положение вещей порождает ряд непроработанных либо проблемных с точки зрения правого регулирования моментов:

- установление четких критериев определения вредоносного (деструктивного) характера подаваемого контента, сложности в механизме реализации уже существующих норм, особенно в глобальном информационном пространстве;

- регламентация способов распространения информации, препятствующая скрытому (манипулятивному) информационному воздействию;

- сопровождение взаимодействия личности с киберпространством и искусственным интеллектом;

- появление новых схем совершения правонарушений в цифровом пространстве и отставание законодательства в контексте фиксации соответствующих запретов;

- вычленение отдельных компонентов в правовом статусе личности, нуждающихся в защите в связи с развитием информационно-коммуникационных технологий (далее

ИКТ). Так, в отдельных странах уже принимаются меры, направленные на регулирование использования цифровых имитаций личности гражданина (дипфейков), созданных с помощью искусственного интеллекта [4].

Таким образом исследуемая сфера нуждается в дальнейшем развитии и совершенствовании с точки зрения государственно-правовой регламентации. При этом следует принимать во внимание следующие нюансы: информационная безопасность личности неразрывно связана с информационной безопасностью государства как компонента национальной безопасности; совершенствование должно протекать с учетом преломления сферы информационной безопасности сквозь призму правого статуса личности; многовекторность существующих угроз предопределяет и необходимость многовекторности средств, а также направлений противодействия, кроме того, принимаемые меры должны отражать и специфику отдельных субъектов защиты (например, несовершеннолетние); область обращения информации на современном этапе постоянно развивается и меняется, зависит от уровня техники и технологий, поэтому правовое регулирование взаимодействия личности с информационным пространством должно соответствовать этим изменениям и быть достаточно гибким. Наибольшую эффективность принимаемые меры будут иметь в условиях функционирования целостного государственно-правового механизма обеспечения информационной безопасности личности.

«Понятие «механизм» широко используется в теоретическом правоведении, где ему придается юридическое значение («правовой механизм»), а его содержание раскрывается как «комплекс юридических средств, последовательно организованных и действующих поэтапно по определенной нормативно заданной схеме». При этом «все элементы правового механизма находятся в логической взаимосвязи». Понятие механизма связывается также с функционированием и взаимодействием государственных институтов – «государственный механизм» [5, с. 99]. Базируясь на теоретических представлениях о сущности государственно-правового механизма в целом, можно сформулировать определение государственно-правового механизма обеспечения информационной безопасности личности. Дефиницией и последующей структурой механизма следует охватить ряд аспектов: объекты защиты, субъекты обеспечения; вызовы и угрозы, средства и способы защиты.

В юридической науке представлены различные концепции механизма обеспечения информационной безопасности в целом либо применительно к интересам личности. «А. А. Тамодлин государственно-правовой механизм обеспечения информационной безопасности личности трактует как систему нормативных, организационных элементов и процедур, гарантирующих состояние защищенности человека в информационной сфере и предоставляющих личности фактическую возможность реализовать свои информационные права и свободы» [6, с. 50].

Ю. И. Литвинова, С. В. Кисс рассматривают «механизм обеспечения информационной безопасности как регламентированную законодательством деятельность уполномоченных субъектов, направленную на охрану и защиту информационной сферы личности, общества и государства от внешних и внутренних угроз и совершенствования мер информационного противодействия» [6, с. 52].

С учетом данного автором в ходе предыдущих исследований определения информационной безопасности личности, а также уже закрепленного в законодательстве определения обеспечения информационной безопасности как «системы мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз» [7] предлагаем следующее определение государственно-правового механизма обеспечения информационной

безопасности личности: система элементов, отражающих деятельность государственных и негосударственных субъектов, последовательно организованных и функционирующих на основе официальных идеологических и нормативных правовых установок, достигнутого уровня развития ИКТ, гарантирующих состояние защищенности личности в информационной сфере.

Механизм обеспечения информационной безопасности личности сложное многокомпонентное понятие. Его составляющие представлены в большинстве теоретических исследований как комплекс организационных, правовых, технических, мер. Полагаем, что структура механизма обеспечения информационной безопасности личности должна включать следующие компоненты: теоретико-идеологический, технический, нормативный, институционально-организационный. Данная комбинация элементов позволит в наибольшей степени гарантировать предупреждение, выявление, пресечение и устранение негативных воздействий на личность в процессе ее взаимодействия с информационной средой.

Так, основу последующего нормативного правового регулирования должна составлять **теоретическая проработка** исследуемой категории. «От правильного теоретического понимания всего того, что регулируется правом и тех условий, в которых осуществляется правовая упорядоченность поведения людей во всех областях их жизни и деятельности, непосредственно зависит эффективность правового воздействия, то есть степень его социально полезной результативности, а значит и продвижение общества по пути прогресса» [1, с. 440–441].

Поскольку теоретическая составляющая предполагает исследование отражения в праве иных социальных регуляторов (морали, религии, нравственности), взаимосвязи права с экономикой, политикой и, соответственно, поиск существующих в обществе ценностей и приоритетов развития, что нашло свое отражение в Основах идеологии белорусского государства, ее можно охарактеризовать как теоретико-идеологическую. Она является базовой в предлагаемом механизме правового регулирования, эффективность принимаемых мер будет зависеть в целом от теоретической проработки категории – информационная безопасность личности – и ее преломления сквозь призму интересов отдельных социальных групп. В рамках теоретической характеристики необходимо: обоснование информационной безопасности применительно к интересам личности, определение ее места в общей системе обеспечения национальной безопасности, а также структуре правового статуса личности; выработка определения, составляющих компонентов информационной безопасности личности, понятия и критериев деструктивного информационного воздействия. Все это ляжет в основу последующей формулировки нормативного определения информационной безопасности личности, которое, по мнению В. А. Шаршуна, «может стать той отправной точкой, от которой будет в дальнейшем происходить формирование соответствующей государственной политики» [3, с. 27].

Автором в ходе ранее проведенных исследований проанализированы обозначенные выше аспекты, сформулировано определение информационной безопасности личности, выделены составляющие данной категории, определены проявления в правовом статусе личности (право личности на безопасность в информационной сфере). Особое внимание уделено ценностно-мировоззренческой основе правового регулирования общественных отношений в области обеспечения информационной безопасности личности. Полагаем, что защита личности от угроз и вызовов в информационном пространстве, как и большинство сфер, связанных с правовым статусом личности, с учетом уже принятых учредительных и стратегических документов должна базироваться на национальной (региональной) модели прав человека.

Техническая составляющая предполагает использование физических, аппаратных, программных и математических средств, обеспечивающих безопасность человека при его взаимодействии с цифровой средой**.** Уровень развития технической составляющей во многом предопределяет необходимость иных средств и методов защиты, в том числе нормативных запретов и ограничений.

Анализируя национальный уровень развития технического компонента в области обеспечения информационной безопасности в целом, следует обратить внимание на недостаточную цифровую зрелость страны, что проявляется в «высокой степени использования организациями импортных аппаратных и программно-аппаратных средств, импортного ПО в цифровой инфраструктуре, нелицензионного ПО, отсутствие понимания всех преимуществ и недостатков при переходе на свободное ПО» [8].

В мировой практике актуальным по-прежнему остается развитие в векторе усиления национального контроля за технической составляющей распространения информации в цифровой среде: Великий китайский файрвол (система контроля за интернетом), многофункциональный сервис обмена информацией в Российской Федерации. Для Республики Беларусь в пределах существующих возможностей развитие может идти по следующим направлениям: создание национального мессенджера, совершенствование программных и программно-аппаратных средств защиты, позволяющих не допустить распространение нежелательной информации, развитие национальных устройств для хранения и передачи информации, в том числе производство национального смартфона, отечественные платформы и приложения.

Нормативный компонент механизма обеспечения информационной безопасности личности представляет собой: *во-первых*, нормативно-правовую фиксацию теоретико-идеологической составляющей. По предложению В. А. Шаршуна, «в Концепции информационной безопасности Республики Беларусь целесообразно закрепить определение термина «информационная безопасность личности, а также определить правовые основы ее обеспечения, которые в последующем должны быть детализированы в иных нормативных правовых актах» [3, с. 29]. Полагаем, что помимо определения информационной безопасности личности подлежит отражению в законодательстве, регулирующем область распространения информации, в последующем – в Информационном кодексе, следующая теоретическая конструкция: право личности на безопасность в информационной сфере и его составляющие: право на защиту от деструктивного информационного воздействия, право на кибербезопасность, право на защиту персональных данных. Также подлежит нормативной фиксации основа правового регулирования общественных отношений в сфере обеспечения безопасности при взаимодействии личности с информационным пространством – национальная модель прав человека. Наиболее приемлемой с учетом уже проходящих в ряде сфер интеграционных процессов, общности исторических, идеологических, религиозных, геополитических факторов, а также с учетом закрепления принадлежности белорусов к восточнославянской цивилизации в Основах идеологии белорусского государства, является разработка Концепции прав человека Союзного государства России и Беларуси. Данный документ должен стать юридическим отражением региональной модели прав человека, как совокупности официальных взглядов на идею прав человека, характеризующих специфику региона с учетом его исторических, ценностно-мировоззренческих, идеологических особенностей, национальных интересов государств-членов, и тем самым определяющих вектор развития сферы прав человека (в том числе права на безопасность в информационной сфере) и его реализацию в законодательстве союзных государств.

Во-вторых, отражение технической составляющей, поскольку правовое регулирование в определенной степени предопределяется техническим развитием и техни-

ческими возможностями по обеспечению безопасности личности в информационном пространстве.

В-третьих, формирование на основе теоретико-идеологического и технического компонентов позитивного регулирования определенных комплексов общественных отношений, а также непосредственных запретов и ограничений. Так, нуждается в совершенствовании правовая регламентация сферы взаимодействия личности с киберпространством. «В действующей нормативной базе отсутствуют четкие определения таких распространенных явлений, как троллинг, кибербуллинг, хэппислепинг, кибersталкинг, преследование в виртуальном пространстве и другие, а также не указаны правовые способы защиты от них» [3, с. 29].

В-четвертых, нормативная составляющая определяет организационно-институциональный компонент с учетом целей и задач разрабатываемого государственно-правового механизма, посредством фиксации правового статуса субъектов обеспечения информационной безопасности личности.

Организационно-институциональный компонент предполагает деятельность прежде всего государственных институтов, для которых соответствующая функция является основной, а также тех, для которых функция обеспечения информационной безопасности реализуется в случае возникновения соответствующих угроз охраняемым интересам личности, и деятельность иных субъектов, что в совокупности должно обеспечивать прогнозирование, выявление внутренних и внешних угроз безопасности личности в информационном пространстве, их нейтрализацию, ослабление фактора угроз, устранение последствий негативного воздействия.

Определение конкретного перечня субъектов, вовлеченных в процесс обеспечения информационной безопасности личности, их функций, задач, определение органа, координирующего их деятельности, выступает актуальным направлением юридической науки, поскольку на сегодняшний день функция обеспечения информационной безопасности рассредоточена по различным структурам. По мнению отдельных исследователей, полномочия государственного регулирования в области обеспечения информационной безопасности личности «могут быть возложены на Оперативно-аналитический центр при Президенте Республики Беларусь или Национальный центр защиты персональных данных Республики Беларусь» [3, с. 28].

Если обратиться к опыту зарубежных государств, где сфера информационной безопасности является одной из ключевых в общей системе обеспечения национальной безопасности (например, Китай), следует отметить, что функция обеспечения информационной безопасности также рассредоточена по различным органам, организациям и иным субъектам, однако есть единая координирующая структура (Коммунистическая партия Китая), акцент в общей системе сделан именно на фильтрации контента (в первую очередь в соответствии с политическими установками) [9].

Полагаем, что в Республике Беларусь с учетом принятых в области обеспечения информационной безопасности нормативных правовых актов, основ идеологии белорусского государства, имеющихся теоретических разработок необходимо на уровне отдельного закона закрепить определение информационной безопасности личности, ее проявления в правовом статусе личности, установить более четкие критерии фильтрации контента, допустимости способов распространения информации, закрепить перечень субъектов, осуществляющих деятельность, направленную на обеспечение информационной безопасности личности, и определить структуру (наиболее оптимальным будет ее создание при ОАЦ), координирующую их деятельность. Поэтому до принятия и вступления в силу Информационного кодекса, считаем целесообразным разработку закона «Об информационной безопасности личности», где следует предметно отразить описанные в исследовании аспекты.

Заключение

Происходящие изменения и усложнения информационных отношений неминуемо сопряжены с появлением новых угроз. С учетом специфики информационной сферы наиболее действенными средствами их нивелирования выступают государственно-правовые средства защиты, а именно государственно-правовой механизм обеспечения информационной безопасности личности.

Его эффективное функционирование предполагает координацию различных правовых и организационных форм деятельности, в связи с чем наиболее оптимальной видится структура, включающая: теоретико-идеологический, технический, нормативный и организационно-институциональный компоненты.

При функционировании механизма должна обеспечиваться оптимизация законодательства под нужды информационного общества, когда с одной стороны обеспечивается право на получение информации, свобода слова и свобода самовыражения, с другой – информационная безопасность личности, общества и государства.

С учетом важности сферы безопасности личности в информационном пространстве в общей системе обеспечения национальной безопасности, она должна быть регламентирована отдельным нормативным правовым актом – законом «Об информационной безопасности личности».

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ***Дробязко, С. Г.*** Избранные труды / С. Г. Дробязко. – Мн. : ЮрСпектр, 2022. – 656 с.

2. О реализации основ идеологии белорусского государства : Директива Президента Респ. Беларусь от 9 апр. 2025 г. № 12 // ЭТАЛОН : информ.-поисковая система (дата обращения: 23.07.2025).

3. ***Шаршун, В. А.*** О некоторых вопросах правового регулирования обеспечения информационной безопасности личности / В. А. Шаршун // Информационная безопасность личности и государства в современном международном праве : материалы круглого стола каф. гос.упр. юрид. фак. Белорус. гос. ун-та, Минск, 12 апр. 2022 г. / Белорус.гос. ун-т ; редкол.: В. С. Михайловский (гл. ред.), Е. Ф. Довгань, Н. О. Мороз. – Мн. : БГУ, 2022. – 298 с. – С. 23–30.

4. Дания собирается бороться с дипфейками, предоставив гражданам авторские права на собственные образ и голос : источник: Общенациональное телевидение – URL: https://ont.by/news/daniya-sobiraetsya-borotsya-s-dipfejkami-predostaviv-grazhdanam-avtorskie-prava-na-sobstvennye-obraz-i-golos – (дата обращения: 19.07.2025).

5. ***Удычак, Ф. Н.*** Государственно-правовой механизм обеспечения национальной безопасности: структурно-функциональный анализ / Ф. Н. Удычак // Вестник Академии экономической безопасности МВД России. – 2010. – № 3. – С. 96–101. – URL: https://cyberleninka.ru/article/n/gosudarstvenno-pravovoy-mehanizm-obespecheniya-natsionalnoy-bezopasnosti-strukturno-funktsionalnyy-analiz/viewer (дата обращения: 19.06.2025).

6. ***Литвинова, Ю. И.*** Механизм обеспечения информационной безопасности государства: теоретико-методологические основы / Ю. И. Литвинова, С. В. Кисс // Юристъ-Правоведъ. – 2020. – № 2 (93). – С. 48–52. – URL: https://cyberleninka.ru/article/n/mehanizm-obespecheniya-informatsionnoy-bezopasnosti-gosudarstva-teoretiko-metodologicheskie-osnovy/viewer (дата обращения: 19.06.2025).

7. О Концепции информационной безопасности Республики Беларусь: Постановление Совета Безопасности Республики Беларусь от 18.03.2019 № 1 // ЭТАЛОН : информ.-поисковая система (дата обращения: 23.06.2025).

8. О Концепции обеспечения суверенитета Республики Беларусь в сфере цифрового развития до 2030 года: Постановление Совета Министров Респ. Беларусь от 31 декабря 2024 г. № 1074 // ЭТАЛОН : информ.-поисковая система (дата обращения: 23.04.2025).

9. ***Ромашкина, Н.*** Эволюция политики КНР в области информационной безопасности / Н. Ромашкина, В. Задремайлова // Пути к миру и безопасности. – 2020. – № 1 (58). – С. 122–138. – URL: https://cyberleninka.ru/article/n/evolyutsiya-politiki-knr-v-oblasti-informatsionnoy-bezopasnosti/viewer (дата обращения: 19.06.2025).

Поступила в редакцию 29.09.2025 г.
Контакты: kuzmenkova@m.msu.by (Кузьменкова Татьяна Николаевна)

Kuzmenkova T. N. **STATE-LEGAL MECHANISM FOR ENSURING PERSONAL INFORMATION SECURITY: STATUS AND DIRECTIONS FOR IMPROVEMENT**

The article is devoted to the analysis of state measures to counter threats arising from the interaction between the individual and the information environment, as well as the vector of their optimization in the context of the functioning of a holistic state-legal mechanism for ensuring the information security of the individual. The study formulates the concept and defines the structure of the proposed mechanism, reflecting the main directions for improving national legislation.

Keywords: state-legal mechanism, personal information security, cybersecurity, national security, human rights, legal status of the individual.