Алхасов Расул Халидбегович
аспирант, заместитель прокурора района
Прокуратура Кировского района г. Махачкалы
г. Махачкала, Республика Дагестан

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ПРЕДМЕТ МЕЖДИСЦИПЛИНАРНОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ: ОТ ТЕОРИИ К ПРАКТИКЕ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация*: вопрос обеспечения информационной безопасности (далее – ИБ) занимает ключевое место в обеспечении безопасности государства и в повседневной жизни человека и общества. В условиях стремительной цифровизации и активного внедрения информационно-телекоммуникационных технологий (далее – ИТТ) возрастает взаимозависимость всех сфер социальной жизни – политики, экономик, правопорядка и т. д. Нарушение безопасности информации ведет к рискам и угрозам не только для пользователей информации, но и для критически важных объектов обеспечения безопасности личности, общества, государства. Решение задач в сфере ИБ возможно лишь при условии применения междисциплинарного подхода, предполагающего взаимодействие юридических, экономических, технических, криминалистических и иных познаний из социогуманитарных сфер.*

Ключевые слова*: междисциплинарный подход, информационная безопасность, правоохранительная деятельность.*

Понятие информационной безопасности в России и в международном правопорядка интерпретируется по-разному, в зависимости от области исследования. Так, если в технической области под ИБ понимается состояние защищенности информационных систем и ресурсов от несанкционированного доступа, их «разрушения» (с технической точки зрения), модификации, блокирование и иные противоправные воздействия, то в юридической сфере это явление приобретает смысл обеспечения правовых гарантий безопасности личности, госу-

дарства и общества: неприкосновенность частной жизни, защита государственной и коммерческой тайны, соблюдение прав субъектов персональных данных [2]. Из этого следует вывод, что информационная безопасность – это интегративное явление, соединяющее правовую, технологическую и социальную составляющие в одном целеполагании – обеспечение надлежащего режима хранения и использования данных и сведений в цифровой среде при помощи права [8].

Обеспечение информационной безопасности на текущем этапе цифровизации экономики, государственного аппарата и жизни общества требует от субъектов обеспечения информационной безопасности принятия решений и осуществление действий в условиях постоянной трансформации возможных угроз [9]. При этом ни одна отрасль самостоятельно не способна обеспечить полноценную защиту цифровой среды без использования смежных отраслей (сфера ИТ – без правовой сферы, и также и наоборот) [6].

Например, установление источника кибератаки невозможно без инструментов анализа сетевого трафика, тогда как закрепление юридической ответственности требует правовой аналитики, с точки зрения уголовного процесса. Особенно это взаимодействие становится важным при возможных проявлениях экстремистского и террористического характера, степень общественной опасности которых крайне деструктивна для безопасности личности, общества и государства [10]. Кроме того, киберугрозы всё чаще носят транснациональный характер, а цифровые следы преступлений могут быть удалены или модифицированы. Для расследования таких преступлений требуется участие специалистов по компьютерной криминалистике, аналитиков, программистов, а также юристов, знающих специфику информационных технологий.

Особое значение здесь приобретают международные стандарты в области информационной безопасности (ISO/IEC 27001 и ISO/IEC 27002), в которых закреплены подходы к управлению информационными рисками и оценке защищенности систем. Однако, наличие таких стандартов, без процесса их внедрения в национальную правовую систему не создает само по себе правовых осно-

ваний их использования, а также необходимых условий для эффективной работы такого стандарта. Для того чтобы эти стандарты действительно работали, они требуют правового обеспечения: только при наличии соответствующих норм законодательства они могут быть использованы государством. При этом остается вопрос соблюдения требований законодательства, возможных коллизий и неопределенностей, которые создают для бизнеса риски привлечения к ответственности в случае наступления той либо иной критической ситуации и неприменением, либо неполным применением требований государственных стандартов и законодательства в угоду международных стандартов.

ИБ представляет собой один из наиболее обсуждаемых современных вопросов. Происходящие нарушения ИБ, например, утечки данных, вмешательство в функционирование государственных сервисов, атаки

на финансовые институты, могут иметь катастрофические последствия для экономики страны и самого государственного устройства в целом. Само по себе обеспечение ИБ – это еще и вопрос стратегического развития государства [1]. Одним из способов обеспечения его обороноспособности, требующим соответствующей институциональной и нормативной базы, подготовленных специалистов и активного взаимодействия между различными отраслями научного познания и социально-ответственного поведения должностных лиц [7], является системный подход.

Использование междисциплинарного (системного) подхода предполагает взаимодействие юристов, специалистов в области информационных технологий, кибернетики, криминалистики, психологии, социологии, экономики и других отраслей научных знаний. Такой синтез позволяет не только оперативно выявлять риски и угрозы, но и более глубоко анализировать мотивации правонарушителей, пытаться действовать «на шаг вперёд» правонарушителя, анализировать и устранять уязвимости цифровой инфраструктуры, а также разрабатывать комплексные меры по обеспечению безопасности государства, граждан, критически важных данных и информации [3], а также любых иных сведений, хранящихся, обрабатываемых и накопляемых посредством цифровых систем.

Междисциплинарное взаимодействие способствует взаимодействию между представителями разных сфер, что важно в условиях, когда правоприменитель должен понимать и использовать выводы технической экспертизы, а специалист по ИТ – учитывать юридические границы допустимости доказательств для обеспечения необходимого уровня законности действий правоохранительных органов. Здесь важны положения современной правовой процессуальной политики, объясняющие не только содержательную сторону процессуальных гарантий, но и методологические основания их реализации в практике правоохранительных органов. В частности, как отмечается в научной литературе, эффективное применение процессуальных норм в условиях цифровизации требует системного подхода, учитывающего как цели правовой политики в целом, так и специфику её процессуального направления [4; 5]. Реализация этих целевых установок невозможна без развития институциональной и образовательной базы, способной обеспечить кадровое обеспечение правоохранительных структур специалистами, владеющими как юридическими, так и техническими аспектами цифровых расследований.

Одним из способов применения междисциплинарного подхода является создание центров компетенций и лабораторий цифровых расследований при правоохранительных органах. Так, в некоторых вузах реализуются образовательные программы по подготовке юристов с ИТ-компетенциями и специалистов по кибербезопасности, владеющих основами права. Министерство внутренних дел Российской Федерации имеет

в своем составе Управление по организации борьбы с противоправным использованием информационного-коммуникационных технологий, активно применяющее в своей практической деятельности междисциплинарный подход при расследовании преступлений. Постоянной проблемой остаётся разрыв между научным знанием и практикой. Даже при наличии квалифицированных экспертов, их участие в уголовных делах ограничивается лишь рамками экспертизы, а не полноценным и компетентным включением в следственные действия.

Осуществив анализ теоретических и практических вопросов деятельности правоохранительных органов в сфере информационной безопасности, необходимо сделать вывод о значимости междисциплинарного подхода в рассматриваемой сфере. В настоящее время практический правовой инструмент обеспечения безопасности государства, позволяющий эффективно противодействовать цифровым угрозам обществу, личности и государству в целом, обеспечить его суверенитет и цифровое развитие. Внедрение междисциплинарного подхода требует системных усилий, в том числе в областях правотворческой деятельности, грамотной организации структуры органов власти, должной кадровой политики и научно-методического обеспечения. В условиях всестороннего междисциплинарного взаимодействия может быть построена современная система информационной безопасности, способная адекватно отвечать на современные риски и угрозы.

Список литературы

1. Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 24.06.2025) «Об информации, информационных технологиях и о защите информации» // СПС КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/ (дата обращения: 01.07.2025).

2. Федеральный закон от 27.07.2006 №152-ФЗ (ред. от 28.02.2025) «О персональных данных» // СПС КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/ (дата обращения: 01.07.2025).

3. Федеральный закон от 26.07.2017 №187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/ (дата обращения: 01.07.2025).

4. Исаев Э.Е. Современное понимание правовой процессуальной политики: теоретико-правовые проблемы / Э.Е. Исаев // Право и государство: теория и практика. – 2023. – №12 (228). – С. 122–124. – DOI 10.47643/1815-1337_2023_12_122. – EDN ODGSCZ.

5. Исаев Э.Е. Цели правовой процессуальной политики: общеправовые и методологические аспекты / Э.Е. Исаев // Ученые записки Казанского университета. Серия: Гуманитарные науки. – 2023. – Т. 165. №6. – С. 7–18. – DOI 10.26907/2541-7738.2023.6.7-18. – EDN UMEYUX.

6. Левкин И.В. Использование методологии междисциплинарности при исследовании цифровых прав: актуальные вопросы / И.В. Левкин // Актуальные вопросы экономики, права и социологии: сборник материалов Всероссийской научно-практической конференции. – Чебоксары: Среда, 2024. – С. 165–167. – EDN BEKJEH.

7. Степаненко Р.Ф. Социально ответственное поведение как фактор устойчивости и стабильности современных государственно-правовых систем / Р.Ф. Степаненко // Государство и право. – 2025. – №6. – С. 7–17. – DOI 10.31857/S1026945225060014. – EDN WBMEKG.

8. Степаненко Р.Ф. Целеполагание в праве: общеправовые и теоретико-методологические проблемы / Р.Ф. Степаненко, Ф.И. Хамидуллина // Государство и право. – 2024. – №10. – С. 45–54. – DOI 10.31857/S1026945224100052. – EDN LJMREG.

9. Толстой А.И. Системотехника обеспечения безопасности объектов в информационной сфере / А.И. Толстой // Вопросы кибербезопасности. – 2024. – №5 (63). – С. 47–57. – DOI 10.21681/2311-3456-2024-5-47-57. – EDN NLAGBE.

10. Шляхтин Е.П. Противодействие деятельности экстремистских организаций и сообществ: актуальные проблемы теории и практики / Е.П. Шляхтин, Р.Ф. Степаненко // Вестник Казанского юридического института МВД России. – 2017. – №2 (28). – С. 100–104. – EDN YRSZPP.