Азаров Кирилл Константинович
магистрант
ФГБОУ ВО «Иркутский национальный
исследовательский технический университет»
оперуполномоченный по особо важным делам
УБК ГУ МВД России
г. Иркутск, Иркутская область

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Аннотация: *в статье анализируются проблемы правового регулирования информационной безопасности органов внутренних дел в условиях цифровизации правоохранительной деятельности. Масштабное внедрение цифровых технологий повышает эффективность процессов, но порождает риски: утечки данных, несанкционированный доступ, нарушение целостности информации. Цель исследования – комплексный анализ законодательства РФ, выявление пробелов и противоречий, обусловленных цифровой трансформацией. Обоснована необходимость совершенствования нормативной базы, стандартизации требований к защите данных и разграничения полномочий. Научная новизна заключается в авторской систематизации правовых механизмов обеспечения информационной безопасности с учетом специфики цифровых вызовов правоохранительной сферы. Сформулированы предложения по повышению эффективности защиты информационных ресурсов и минимизации рисков.*

Ключевые слова: *информационная безопасность, органы внутренних дел, цифровизация, правовое регулирование, цифровая трансформация, киберугрозы, нормативная база.*

Цифровизация деятельности органов внутренних дел осуществляется в рамках реализации комплекса государственных стратегий, программ и концептуальных документов, направленных на развитие информационного общества и

обеспечение национальной безопасности Российской Федерации. К их числу относятся Стратегия развития информационного общества в Российской Федерации [6], Доктрина информационной безопасности Российской Федерации, а также государственные и ведомственные программы цифровой трансформации, реализуемые МВД России [5].

Указанные документы закрепляют приоритет внедрения информационных технологий в деятельность правоохранительных органов, рассматривая цифровые инструменты как ключевой фактор повышения эффективности управления, оперативно-розыскной и процессуальной деятельности, а также профилактики правонарушений.

Реализация данных стратегических установок объективно приводит к существенному увеличению объёмов обрабатываемой информации, усложнению структуры информационных потоков и изменению характера информационного взаимодействия как внутри системы органов внутренних дел, так и на межведомственном уровне.

Современные цифровые процессы предполагают непрерывный обмен данными между различными подразделениями, автоматизацию аналитических процедур, интеграцию разнородных информационных ресурсов, а также использование электронных форм фиксации, хранения и передачи служебных сведений. В результате, возрастает не только ценность информации как ресурса, но и уровень рисков, связанных с её утратой, искажением либо неправомерным использованием.

В практической деятельности органы внутренних дел используют разветвлённую систему ведомственных информационных ресурсов и автоматизированных учётов, включающую базы данных оперативно-розыскного назначения, криминалистические и дактилоскопические учёты, миграционные и регистрационные реестры, информационные системы административной и уголовно-процессуальной деятельности.

Эти информационные массивы аккумулируют значительные объёмы персональных данных, сведений ограниченного доступа, а также информации,

составляющей служебную тайну. Нарушение установленного режима защиты таких данных способно повлечь тяжёлые последствия, выражающиеся в подрыве эффективности расследования преступлений, нарушении прав и законных интересов граждан, дискредитации органов внутренних дел и снижении доверия общества к правоохранительной системе.

Функционирование указанных информационных систем напрямую зависит от устойчивости и полноты правового режима защиты информации. Такой режим должен обеспечивать разумный баланс между необходимостью оперативного доступа к сведениям для решения служебных задач и обязанностью государства гарантировать соблюдение конституционных прав граждан на неприкосновенность частной жизни, защиту персональных данных и тайну частной информации [1].

В условиях цифровизации данный баланс приобретает особую значимость, поскольку чрезмерная формализация процедур может негативно сказаться на оперативности правоохранительной деятельности, тогда как недостаточная правовая регламентация создаёт условия для злоупотреблений и правовых конфликтов.

Действующее федеральное законодательство в сфере информационной безопасности формирует преимущественно рамочную модель правового регулирования [4]. Федеральный закон «Об информации, информационных технологиях и о защите информации» закрепляет базовые принципы защиты информации, включая требования к обеспечению её конфиденциальности, целостности и доступности, однако не содержит специальных норм, учитывающих специфику правоохранительной деятельности и повышенный уровень рисков, характерных для системы органов внутренних дел [2].

Аналогичным образом Федеральный закон «О персональных данных» [3] устанавливает универсальные требования к обработке персональной информации, которые не всегда коррелируют с особыми условиями работы правоохранительных органов, предполагающими необходимость быстрого доступа к данным, их систематического обновления и межведомственного обмена в рамках реализации публично-правовых функций.

Ведомственное правовое регулирование МВД России призвано компенсировать указанные ограничения федерального законодательства, однако на практике оно отличается значительной фрагментарностью и отсутствием единого системного подхода. Нормативные правовые акты, регламентирующие вопросы защиты информации, эксплуатации информационных систем, разграничения уровней доступа, контроля за действиями пользователей и ответственности должностных лиц, зачастую разрабатываются разрозненно, без учёта комплексного характера информационной безопасности. В результате, отдельные элементы системы защиты функционируют изолированно, что снижает общий уровень защищённости ведомственных информационных ресурсов и усложняет координацию между подразделениями.

Особую актуальность в условиях цифровизации приобретает проблема правового регулирования доступа сотрудников органов внутренних дел к информационным ресурсам. Расширение цифровых возможностей неизбежно сопровождается увеличением числа пользователей, наделённых правом работы с конфиденциальной информацией, что повышает риск несанкционированного использования данных, превышения служебных полномочий и утечек информации по вине человеческого фактора [7, с. 561].

Практика показывает, что значительная часть инцидентов информационной безопасности связана не с техническими сбоями, а с недостаточной правовой регламентацией процедур доступа, отсутствием эффективных механизмов фиксации действий пользователей и формальным подходом к контролю за соблюдением установленных требований.

В этих условиях возникает объективная необходимость дальнейшего развития правового регулирования, направленного на детализацию процедур доступа к информационным ресурсам, установление чётких критериев разграничения полномочий, внедрение обязательных механизмов учёта и аудита действий пользователей, а также усиление юридической ответственности за нарушения в сфере информационной безопасности.

Совершенствование нормативной базы в данном направлении должно учитывать специфику правоохранительной деятельности, динамику цифровых процессов и необходимость обеспечения устойчивости информационной инфраструктуры органов внутренних дел в условиях возрастающих киберугроз.

Правоприменительная практика свидетельствует о том, что в деятельности органов внутренних дел регулярно фиксируются случаи превышения должностных полномочий, несанкционированного обращения к ведомственным информационным ресурсам, а также утечки служебной информации, обусловленные так называемым человеческим фактором. Подобные нарушения проявляются, в частности, в неправомерном использовании служебных баз данных в личных целях, передаче сведений третьим лицам, получении информации вне рамок служебной необходимости, а также в несоблюдении установленных правил хранения и обработки данных. Особую опасность представляют ситуации, когда доступ к информации используется не для выполнения служебных задач, а в корыстных или иных противоправных целях, что наносит ущерб как интересам государства, так и правам граждан [8, с. 19].

Несмотря на то, что действующее законодательство предусматривает дисциплинарную, административную и уголовную ответственность за нарушение требований информационной безопасности, превентивные правовые механизмы в данной сфере остаются недостаточно развитыми. Основной акцент правового регулирования по-прежнему делается на меры реагирования уже после совершения нарушения, тогда как профилактика противоправного поведения сотрудников в цифровой среде остаётся второстепенной, что свидетельствует о необходимости смещения правового фокуса с карательных мер на предупреждение правонарушений, что возможно лишь при условии нормативного закрепления более детализированных процедур контроля доступа к информационным системам и обязательной фиксации всех действий пользователей.

Особое значение в этом контексте приобретает правовое регулирование механизмов аутентификации, авторизации и учёта действий сотрудников при работе с ведомственными информационными ресурсами. В отсутствие чётко

регламентированных требований к разграничению прав доступа и обязательному ведению журналов действий пользователей затрудняется выявление виновных лиц и установление причин инцидентов информационной безопасности. Следовательно, нормативное закрепление обязательных процедур логирования, регулярного анализа действий пользователей и правового аудита информационных систем должно рассматриваться как один из ключевых элементов обеспечения информационной безопасности органов внутренних дел.

Значительное влияние на общее состояние защищённости информации оказывает уровень правовой регламентации межведомственного информационного взаимодействия. В условиях цифровизации органы внутренних дел активно обмениваются сведениями с судами, органами прокуратуры, налоговыми органами, Росреестром, органами социальной защиты и иными государственными структурами. Такой обмен осуществляется в электронном виде и предполагает передачу значительных массивов данных, в том числе персональной и служебной информации.

При этом правовые основания, порядок, объём и условия передачи сведений нередко регламентируются разрозненными нормативными актами, что затрудняет обеспечение единых требований к защите информации.

Отсутствие унифицированных стандартов правового регулирования межведомственного информационного взаимодействия создаёт риски утраты контроля над передаваемой информацией, нарушения режима конфиденциальности и неопределённости ответственности за возможные утечки данных.

В ряде случаев неясно, какой именно орган несёт ответственность за сохранность информации после её передачи, а также какие меры защиты должны применяться на каждом этапе информационного обмена, что указывает на необходимость разработки единых правовых подходов к регулированию межведомственного электронного взаимодействия с участием органов внутренних дел.

Не менее значимой является проблема правового обеспечения защиты информации при привлечении внешних подрядчиков и использовании программных решений сторонних разработчиков. В условиях реализации политики импортозамещения и обеспечения цифрового суверенитета МВД России

взаимодействует с различными организациями, осуществляющими разработку, внедрение, сопровождение и модернизацию ведомственных информационных систем. При этом такие организации в ряде случаев получают доступ к технической инфраструктуре и, опосредованно, к служебной информации, что объективно повышает уровень рисков информационной безопасности.

Действующий правовой режим допуска внешних подрядчиков к работе с информационными ресурсами органов внутренних дел нуждается в дополнительной детализации.

В частности, требуется более чёткое нормативное закрепление требований к сертификации программных средств, порядку допуска специалистов к работам, связанным с обработкой информации ограниченного доступа, а также установление расширенных мер юридической ответственности за нарушение режима информационной безопасности. Недостаточная определённость данных вопросов может привести к снижению уровня защищённости информационных систем и возникновению правовых коллизий [9, с. 17].

Анализ правоприменительной практики позволяет сделать вывод о том, что значительная часть инцидентов информационной безопасности в органах внутренних дел обусловлена не столько техническими сбоями, сколько недостатками правового регулирования и организационного обеспечения.

К числу таких недостатков относятся формальный подход к обучению сотрудников требованиям информационной безопасности, отсутствие регулярной оценки правовых и информационных рисков, а также несвоевременное обновление нормативных правовых актов с учётом динамичного развития цифровых технологий.

В условиях быстрого технологического прогресса правовое регулирование нередко не успевает адаптироваться к новым формам угроз, что снижает его эффективность.

В этой связи представляется обоснованным вывод о необходимости перехода от фрагментарного к системному правовому регулированию обеспечения информационной безопасности органов внутренних дел.

Такая система должна основываться на единых принципах, включать чёткое распределение полномочий и ответственности между субъектами обеспечения информационной безопасности, стандартизированные требования к защите информации, а также действенные механизмы правового контроля и ответственности.

Особое значение при этом приобретает гармонизация ведомственного регулирования с федеральными нормами и национальной системой технического регулирования в сфере информационной безопасности [10, с. 18].

В качестве одного из перспективных направлений совершенствования правового регулирования целесообразно рассматривать разработку комплексного ведомственного нормативного правового акта, закрепляющего основы обеспечения информационной безопасности в системе МВД России с учётом процессов цифровизации.

Такой акт мог бы выполнять роль системообразующего документа, определяющего принципы, цели, задачи и механизмы защиты информации, координировать применение иных нормативных актов и стандартов, а также служить ориентиром для правоприменительной практики и ведомственного контроля.

Подводя итог, следует подчеркнуть, что цифровизация правоохранительной деятельности неизбежно трансформирует требования к правовому регулированию обеспечения информационной безопасности органов внутренних дел. Эффективное функционирование правоохранительной системы в цифровой среде возможно исключительно при условии опережающего и системного развития правовых механизмов защиты информации.

В противном случае технологический прогресс будет сопровождаться ростом правовых, организационных и информационных рисков, способных негативно отразиться на реализации функций органов внутренних дел, уровне доверия общества к правоохранительным органам и состоянии общественной безопасности в целом.

Список литературы

1. Конституция Российской Федерации: принята всенародным голосованием 12 дек. 1993 г.: (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ) // Собрание законодательства РФ. – 2020. – №11. – Ст. 1416.

2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ: (ред. действующая) // Собрание законодательства РФ. – 2006. – №31 (ч. I). – Ст. 3448.

3. Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ: (ред. действующая) // Собрание законодательства РФ. – 2006. – №31 (ч. I). – Ст. 3451.

4. Федеральный закон «О безопасности» от 28.12.2010 №390-ФЗ: (ред. действующая) // Собрание законодательства РФ. – 2011. – №1. – Ст. 2.

5. Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 05.12.2016 №646 // Собрание законодательства РФ. – 2016. – №50. – Ст. 7074.

6. Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы: утв. Указом Президента РФ от 09.05.2017 №203 // Собрание законодательства РФ. – 2017. – №20. – Ст. 2901.

7. Бачило И.Л. Информационное право: учебник для вузов / И.Л. Бачило. – 5-е изд., перераб. и доп. – М.: Юрайт, 2021. – 576 с.

8. Кашанин А.В. Правовое обеспечение информационной безопасности: монография / А.В. Кашанин. – М.: Норма, 2020. – 304 с.

9. Талапина Э.В. Цифровое государство: право и технологии: монография / Э.В. Талапина. – М.: Юстицинформ, 2019. – 352 с.

10. Воронин С.А. Информационная безопасность в деятельности органов внутренних дел / С.А. Воронин, В.Н. Петров // Административное и муниципальное право. – 2022. – №4. – С. 15–24.