УДК 342.9

Караваев Александр Александрович
кандидат юридических наук, доцент кафедры административной деятельности органов внутренних дел,
Воронежский институт МВД России.
ferrari49@yandex.ru
Щеглов Евгений Николаевич
Адвокат,
Воронежская областная коллегия адвокатов.
ferrari49@yandex.ru
Alexander A. Karavaev
Candidate of Legal Sciences,
Associate Professor of the Department
of Administrative Activities of Internal Affairs Bodies,
Voronezh Institute of the Ministry of Internal Affairs of Russia.
ferrari49@yandex.ru
Evgeny N. Shcheglov
Advocate.
Voronezh Regional Bar Association.
ferrari49@yandex.ru

ТЕОРЕТИКО-ПРАВОВОЙ АНАЛИЗ ОТДЕЛЬНЫХ ПОЛОЖЕНИЙ ДОКТРИНЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ИСПОЛНИТЕЛЬНЫХ ОРГАНОВ ВЛАСТИ

THEORETICAL AND LEGAL ANALYSIS OF SEPARATE PROVISIONS OF THE INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION IN THE SPHERE OF PROTECTING THE INFORMATION RESOURCES OF THE EXECUTIVE AUTHORITIES

Аннотация*. В статье производится исследование официальных взглядов на вопросы обеспечения информационной безопасности, изложенных в Доктрине информационной безопасности Российской Федерации применительно к автоматизированным электронным ресурсам органов внутренних дел. Исследуются актуальные задачи и направления обеспечения безопасного оборота конфиденциальной информации в органах исполнительной власти. Обозначаются отдельные угрозы электронному информационному пространству органов внутренних дел.*

Ключевые слова: *информационная безопасность, конфиденциальные сведения, правонарушение, профилактическая информационных угроз, информационные риски, хранение конфиденциальной информации, информационных банки данных.*

Annotation. *The article examines the official views on the issues of information security, set out in the Doctrine of Information Security of the Russian Federation in relation to the automated electronic resources of the internal affairs bodies. The current tasks and directions of ensuring the safe circulation of confidential information in the executive authorities are investigated. Individual threats to the electronic information space of the internal affairs bodies are indicated.*

Key words: *information security, confidential information, delinquency, preventive information threats, information risks, storage of confidential information, information databanks.*

Актуальность исследования информационных ресурсов федеральных органов исполнительной власти подчеркивается рядом факторов. Во-первых, первично орган власти позиционируется индивидом, как нечто охранительное в части касающейся его прав и свобод, имеющих нормативное регламентирование. Во-вторых, распространение Covid-19 для населения России привнесло определенные новеллы в части организации работы государственных органов, учреждений, должностных лиц. В-третьих, приоритетно обозначена роль технологий «удаленного доступа» практически в каждой сфере жизни общества. Следовательно, возрастает значение дистанционных инструментов исполнения должностных обязанностей. Информационные ресурсы в данном контексте представляются одним из центральных элементов системы обеспечения деятельности федеральных органов исполнительной власти.

Доктринальное осмысление информации происходит в научном сообществе достаточно долгий временной период, при этом «цифровизация» (переход к электронным носителям) отмечается зачастую сложным процессом с позиции организации защиты. Подобное течение научной мысли обусловлено рядом практических составляющих. В электронных информационных ресурсах увеличивается сегмент накопления, хранения, унификации, оперативности доступа, реализация его дистанционным способом. Бесспорным, с позиции научного осмысления, представляется использование актуальных информационных технологий в деятельности органов исполнительной власти как современного метода оказания дистанционных услуг населению и обслуживания его интересов. Однако, любой прогресс помимо позитивных тенденций может формировать отдельные правовые риски, либо создавать конкретные угрозы реализации отдельных прав (свобод) граждан. В данном контексте, такими деструктивными факторами могут выступать неправомерный доступ третьих лиц к охраняемым законом тайнам.

Иллюстрировать обозначенную концепцию, по мнению авторов, может оборот конфиденциальных сведений в информационных ресурсах различных органов исполнительной власти. К примеру, накопление различных персональных данных, личной, семейной, отдельной коммерческой тайны в информационных банках органов внутренних дел происходит на постоянной

основе. Обозначенный ресурс необходим полиции для качественного исполнения возложенных действующим законодательством обязанностей. Переход к электронным банкам упрощает доступ фактического правоприменителя к необходимым сведениям и сокращает временные затраты, которые могли понадобиться для исполнения организационных предписаний, определенных для получения доступа к конкретной информации, хранящейся на бумажном носителе. Таким образом, путем сокращения временных затрат возрастает показатель оперативности принимаемых решений, реализуемых действий, что в, определенном контексте, положительно влияет на процентное соотношение раскрываемости противоправных деяний и привлечение виновных к установленной законом ответственности.

Негативной составляющей обозначенного процесса, по мнению авторов, является возможность распространения широкого спектра конфиденциальной информации среди неопределенного круга лиц, которые могут не иметь доступа к охраняемым сведениям с позиции действующего законодательства. Охрана информации в электронном цифровом формате имеет ряд отличительных особенностей. К ним относится системность, практичность, актуальность, техническая грамотность, нормативная правовая регламентированность, организационная обеспеченность и некоторые другие. Исключительно комплексное использование охранительного инструментария позволит добиться его качественной реализации. Поскольку важным характеризующим элементом любой охранительной системы является сбалансированность.

Одним из центральных документов, определяющим видение законодателя отдельных элементов информационной безопасности является Доктрины информационной безопасности Российской Федерации [1]. Данный документ является результатом научного, правового, организационного осмысления современных информационных угроз, а также приоритетных задач и направлений деятельности в исследуемой сфере. Нормотворец в обозначенном документе использует формулировку «система официальных взглядов» на обеспечение безопасности в сфере информации. Такая позиция, представляется нам, вполне оправданной, поскольку доктринальное осмысление любой проблемы предполагает формирование широкой научной позиции, на которой впоследствии могут быть построены частные научные изыскания отдельных исследуемых сфер. В рамках статьи, представляется актуальным, рассмотреть отдельные положения Доктрины, поскольку именно они впоследствии определят вектор нормативного правового регулирования отдельных сфер информационной защиты.

Понятие «обеспечение информационной безопасности» представленное в Доктрине информационной безопасности Российской Федерации, по мнению авторов, представляет определенный научный интерес. Применительно к проблеме защиты сведений в автоматизированных информационных системах органов внутренних дел, речь должна идти о правовых, организационных, научно-технических, кадровых и

экономических мерах. Ключевым понятием для категории «обеспечение информационной безопасности» является взаимоувязанность. Это всегда комплекс мер, которые должны быть разумно сбалансированы между собой.

Наличие четкой системы запретов и обязанностей субъектов, использующих информационную систему, без обеспечения должного уровня технической защиты информации не может обеспечить реальную защиту этой системы и, наоборот, никакая техническая система защиты информации без системы локального нормативного правового регулирования не сможет реально защитить информацию [2].

Следовательно, в рамках вопроса обеспечения сохранности сведений в автоматизированных системах органов внутренних дел применение разведывательных, контрразведывательных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления на постоянной основе представляется, в определенном контексте, чрезмерно затратным фактором. Поскольку мероприятия подобного порядка потребуют значительного количества ресурсной базы различных подразделений государственного аппарата задействованных в обозначенном направлении деятельности.

Обратим внимание еще на ряд положений Доктрины информационной безопасности Российской Федерации. Деятельность органов внутренних дел и полиции в ней специально не выделяется. Она входит в более общий блок общественных отношений – информационную безопасность в области государственной и общественной безопасности.

Анализируя вышеприведенное положение, авторы хотели бы высказать следующее, при наличии ядерного и иных видов оружия массового поражения, действующих механизмов политического, экономического и военного сдерживания на международном уровне ни одна из развитых стран мира или их коалиция не позволит себе начать полномасштабную военную агрессию. Это чревато необратимыми последствиями. Но если невозможно разрушить государственность на какой-либо территории исключительно военным путем, ее можно попытаться уничтожить или ослабить, используя внутренние силы и противоречия. Именно на это и направлено, в конечном счете, информационное противоборство между мировыми державами. Роль полицейской информации, сконцентрированной в автоматизированных информационных системах, в военном противостоянии крайне низка, но она весьма повышается в информационно-политическом противостоянии, когда в ход идут аргументы коррумпированности власти, осуществления ею противоправных действий в отношении оппозиционно настроенных граждан и т.д.

Примерами обозначенной деятельности, на практике, могут быть политические устремления различных оппозиционных сил, которые пытаются спровоцировать массовые народные волнения, направленные на изменение действующего политического курса, смены руководства страны, изменение конституционного устройства государственного аппарата. Подобная деятельность реализуется этапами, имеет зачастую зарубежное

финансирование, целевые «условно легитимные» задачи, декламируемые широкой общественности в конечном итоге, подменяются противоправными. Граждане, вовлеченные в подобную деятельность под различными предлогами обманным путем, после разоблачения организаторов несут юридическую ответственность в соответствии с действующим законодательством.

По нашему мнению, организаторы подобных акций, заплатят значительную сумму, если в их распоряжение попадет банк оперативной информации в отношении государственных служащих регионального или федерального уровня, содержащий негативные сведения об их деятельности, в том числе связанные со злоупотреблением должностными полномочиями. Такая информация, пусть даже не имеющая должного уровня достоверности, дает повод для шантажа, склонения к выполнению заданий, направленных на подрыв суверенитета государства.

Следующим уровнем информационных угроз является так называемая компьютерная преступность, которая постоянно активизируется в кредитно-финансовой сфере, а также посягает на частную жизнь, личную и семейную тайну граждан, коммерческую тайну корпоративных организаций и т.д.

Доктрина информационной безопасности Российской Федерации в своем содержание раскрывает основные направления обеспечения информационной безопасности в области государственной и общественной безопасности (статья 23), в рамках данной статьи, отметим ряд авторских комментариев относительно обозначенных положений.

Применительно к пункту «а» следует отметить, что в настоящий период времени отмечается активнейшее использование информационных технологий, прежде всего возможностей сервисов сети Интернет (Skype, WhatsApp, Telegram и др.), а также так называемых «социальных сетей», для распространения идей экстремистского содержания, привлечения сторонников, организации демонстраций, массовых беспорядков и т.п. Задача полиции в данном направлении состоит в накоплении сведений о субъектах данной деятельности, защите своих собственных информационных ресурсов, своевременном реагировании на активизацию использования сетей для подготовки противоправных действий.

Дополнительная угроза, в рамках обозначенной деятельности, зачастую заключается в том, что к ней привлекаются несовершеннолетние лица. Данные социальные индивиды легко поддаются внушению ложными идеалами поскольку не имеют достаточного жизненного опыта. Привлечение несовершеннолетних, в широком понимании, создает фактическую угрозу будущему национальному развитию, поскольку насаждение идеологии правого нигилизма в «неокрепшем» сознание деструктивно сказывается на процессах правового воспитания, развития социализированной личности [3]. К примеру, возможно рассмотреть социальную ситуацию на территории государства Украина. Непосредственное вовлечение молодежи в националистические движения повлекло массовые беспорядки, нарушение прав и свобод граждан, причинение различных видов ущерба.

Применительно к пункту «в» задача полиции состоит в активном участии в мероприятиях по повышению защищенности систем автоматизированного управления транспорта, промышленных объектов, объектов энергетического комплекса от деструктивных воздействий на эти системы.

Прогнозируемые риски, в данном сегменте, государственной деятельности достаточно сложно переоценить, поскольку ущерб техногенных катастроф в исторической ретроспективе всегда сопровождался значительными социальными потерями. В некоторых случаях, последствия случившихся аварий на объектах промышленности еще долгий период времени влекут деструктивные последствия экологического характера на данной территории и создают условия для необходимости поиска новой территории для жизни местному населению. Подобная деятельность постоянно сопровождается значительными затратами из государственного и муниципального бюджета, ориентированными на создание благоприятных условий для жизни людей оставшихся без какой-либо недвижимости пригодной для проживания.

Применительно к пункту «г» следует отметить, что по мере повышения уровня автоматизации в управлении органами внутренних дел уязвимость ведомственной информационной инфраструктуры также неизбежно увеличивается. Причем, помимо деструктивной деятельности зарубежных спецслужб, воздействие на информационные ресурсы полиции возможно и внутри страны, как с целью получения интересующей информации, ее искажения или уничтожения, так и с целью дезорганизации работы автоматизированных систем.

Система обеспечения безопасности информационных ресурсов органов внутренних дел, в определенном контексте, является интересным объектом для посягательства злоумышленников. Первичной целью возможно рассмотреть желание правонарушителя похитить сведения для организации шантажа, вымогательства и прочих противоправных деяний в отношении третьих лиц (фигурантов информационной системы). Однако, в качестве вторичных целей возможно рассмотреть желание правонарушителя изменить, исказить, удалить ряд сведений о себе, которые были внесены в электронную информационную систему в связи с совершением противоправных действий данным индивидом. Безусловно, что на обозначенных двух направлениях круг целевых устремлений правонарушителя не может быть исчерпан и на практике он может быть значительно шире.

Применительно к пункту «ж» следует отметить, что органы внутренних дел в целом и полиция как их составная часть являются аккумуляторами огромного количества сведений ограниченного доступа, существенная часть из которых составляет государственную тайну. Отсюда вытекает необходимость принятия целого комплекса мер по защите информации. И если в отношении сведений на бумажных носителях правовое регулирование данных отношений сложилось давно, а также имеется устоявшаяся

административная практика в этом вопросе, то в отношении автоматизированных банков данных проблема защиты информации по-прежнему имеет место.

Рассмотрев некоторые вопросы обеспечения информационной безопасности, авторы хотели бы констатировать, что данное направление государственной деятельности является весьма широким и ему в современных общественно-политических реалиях придается большое значение. Именно поэтому, комплексное сбалансированное решение охранительных задач информационной безопасности невозможно без научного, практического, нормативного правового осмысления современных реалий. Представляется, что нормативная правовая деятельность государственного аппарата в контексте информационной безопасности электронных информационных ресурсов органов внутренних дел нуждается в дополнительной проработке с позиции актуальных рисков, данную деятельность необходимо основывать на системном мониторинге угроз и правоприменительной практике.

ЛИТЕРАТУРА

1. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 декабря 2016 года № 646 // Собр. законодательства Рос. Федерации. – 2016. – № 50. – Ст. 7074.

2. Фатьянов А.А. Правовое обеспечение безопасности информации. – М., – 2001. – С. 48.

3. Занина Т.М. Зарубежный опыт организации профилактической работы в отношении несовершеннолетних правонарушителей / Т.М. Занина, М.В. Бутова // Общество и право. – 2019. – № 2 (68). – С.97-101.

REFERENCES:

1. On the approval of the Doctrine of information security of the Russian Federation: decree of the President of the Russian Federation of December 5, 2016 No. 646 // Collected. legislation Ros. Federation. - 2016. - No. 50. - Art. 7074.

2. Fatyanov A.A. Legal security of information. - M., - 2001. - S. 48.

3. Zanina T.M. Foreign experience in organizing preventive work in relation to juvenile offenders / T.M. Zanina, M.V. Butova // Society and Law. - 2019. - No. 2 (68). - S.97-101.