Воронежский институт МВД России

Т. М. Занина
А. А. Караваев

АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБОРОТА И ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Монография

Воронеж
2018

ББК 67.401.133
З-27

Рецензенты:
А. А. Фатьянов, заведующий кафедрой государственно-правовых и уголовно-правовых дисциплин Российского экономического университета имени Г. В. Плеханова, академик РАЕН, доктор юридических наук, профессор;
Р. В. Никулин, начальник межмуниципального отдела МВД России на режимных объектах Воронежской области;
Н. С. Куликова – начальник отдела информации и общественных связей ГУ МВД России по Воронежской области, кандидат юридических наук.

Рукопись рассмотрена и рекомендована к изданию на заседании редакционно-издательского совета Воронежского института МВД России протокол № 12 от 19.12.2017.

Занина Т. М.
З-27 Административно-правовое регулирование оборота и защиты конфиденциальной информации в органах внутренних дел : монография / Т. М. Занина, А. А. Караваев. – Воронеж : Воронежский институт МВД России, 2018. – 104 с.

ISBN 978-5-88591-573-1

В монографии рассмотрены теоретические и практические аспекты оборота конфиденциальной информации в органах внутренних дел, а также особенности административной ответственности по данным составам правонарушений. Особое внимание уделяется электронным базам данных, которые содержат конфиденциальную информацию, используемую сотрудниками органов внутренних дел.

Предназначена для профессорско-преподавательского состава, курсантов и слушателей юридических факультетов, сотрудников органов внутренних дел.

З 1203021100-02 34(II) -18 ББК 67.401.133
221-18

ISBN 978-5-88591-573-1

Содержание

ВВЕДЕНИЕ

Информационные технологии, являющиеся материальной основой для формирования и практического использования информационных ресурсов, продолжают развиваться настолько стремительно, что за ними не успевает ни одна иная отрасль экономики.

Проникновение информационных технологий во все сферы жизни общества, их вхождение, по сути, в каждый дом среди многочисленных положительных моментов имеет своим следствием и негативные. Современные системы поиска и обработки информации позволяют осуществлять глобальный контроль над коммуникациями не только органов публичной власти, но и сотен миллионов граждан, накапливая и анализируя многочисленную информацию о них.

Эта сложная поисковая работа является технологически чрезвычайно сложной и под силу только крупнейшим государствам, поэтому устремления субъектов меньшей величины направлены прежде всего на получение доступа к уже организованным информационным массивам, а именно к банкам данных.

Полезно обеспечивать сохранность любой информации, накопленной в автоматизированной системе, особое значение приобретает защита тех сведений, доступ к которым ограничивается по объективным причинам. Среди таких сведений главенствующее положение занимает государственная тайна. Однако помимо нее существует более широкий класс сведений, именуемый конфиденциальной информацией, которые также подлежат защите, и в ряде случаев ценность такой информации приближается к ценности сведений, составляющих государственную тайну.

Органы внутренних дел в силу выполнения ими определенных задач, прежде всего связанных с обеспечением общественной безопасности и борьбой с преступностью, являются аккумулятором огромного числа сведений конфиденциального характера, поступающих к ним из внешней среды, а также сами создают значительное число сведений о своей деятельности, которые не подлежат открытому распространению, но в силу объективных причин не могут быть отнесены к государственной тайне. Поэтому изучение проблем, связанных с отнесением сведений к категории конфиденциальной информации и упорядочением их оборота, на примере органов внутренних дел имеет весьма актуальное значение.

Данная проблема имеет также иной ракурс рассмотрения – с позиций обеспечения прав человека и гражданина. Выполняя поставленные задачи, органы внутренних дел в законодательно очерченных рамках, но тем не менее весьма существенно вторгаются в частную сферу жизни граждан, накапливая о них многочисленные сведения личного и коммерческого характера. Данная деятельность направлена прежде всего на решение про-

блем обеспечения общественной безопасности и осуществление борьбы с преступностью, однако вытекающие из этого широкие правомочия по сбору и обработке информации накладывают на органы внутренних дел не менее широкий комплекс обязанностей по обеспечению защиты указанной информации от противоправного распространения или использования. Система защиты информации конфиденциального характера в органах внутренних дел, имеющая правовую, организационную и техническую составляющие, должна гарантировать исключение возможности неконтролируемого доступа или утечки защищаемых сведений, а также искажения их содержания.

Окружающая нас действительность стремительно изменяется во многом за счет активного развития информационных технологий. Многое из того, что вчера рассматривалось как последнее достижение, сегодня уже воспринимается как нечто устаревшее. Общая идеология развития государственного управления в нашей стране заключается в стремлении максимально автоматизировать многие управленческие процессы, исключив или существенно ограничив участие в их осуществлении человека.

Объединение вышеприведенных теоретических посылок применительно к проблемам информационного обеспечения деятельности органов внутренних дел позволяет утверждать, что уже в среднесрочной перспективе потребуется не только доступ к банкам данных органов внутренних дел из некоторой совокупности стационарных точек, но и мобильный, и даже онлайн-доступ, который, естественно, должен осуществляться по защищенным каналам связи, с абсолютно точной идентификацией и аутентификацией пользователей.

Все вышеизложенное предопределяет актуальность проведения монографического исследования, посвященного правовому регулированию оборота и защиты сведений конфиденциального характера в органах внутренних дел, которое в основном осуществляется нормами административного права.

§ 1. Эволюция правового регулирования в отношении сведений конфиденциального характера в Российской Федерации

Можно сказать, что системное появление в российском законодательстве правовой категории «конфиденциальная информация» связано с принятием в 1994 году Федерального закона «Об информации, информатизации и защите информации»[1], который внес определенное упорядочение в градацию информационных ресурсов по категориям доступа. В соответствии с п. 2 ст. 10 данного закона, «документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную».

Такое разделение являлось системным и ознаменовало собой новый этап в развитии правового регулирования ограничения в доступе к информации.

В тот период времени термин «конфиденциальность (конфиденциальный)» был относительно новым для отечественного законодательства. Самым ранним по дате актом, который авторскому коллективу удалось обнаружить в нормативном массиве, использовавшем данную категорию, являлось Постановление СМ СССР от 16.08.1990 № 835 «О мерах по демонополизации народного хозяйства»[2], где предписывалось не допускать таких проявлений недобросовестной конкуренции, как самовольное использование или разглашение конфиденциальной научно-технической, производственной или торговой информации.

Справедливости ради следует отметить, что на уровне надзорных правоприменительных актов данный термин был использован несколькими месяцами ранее и в более широком смысле. В Заключении Комитета конституционного надзора СССР от 21.06.1990 № 2-2 «О несоответствии норм законодательства, исключающих для ряда категорий работников судебный порядок рассмотрения индивидуальных трудовых споров, положениям Конституции СССР, законов СССР, международных актов о правах человека»[3] было отмечено следующее:

«Настоящее Заключение комитета не исключает возможности установления в законе иного порядка рассмотрения споров по вопросам

---

[1] Об информации, информатизации и защите информации : федеральный закон от 20.02.1995 № 24-ФЗ // СПС «Консультант Плюс».

[2] О мерах по демонополизации народного хозяйства : постановление СМ СССР от 16.08.1990 № 835 // Собр. постановлений СССР. – 1990. – № 24. – Ст. 114.

[3] О несоответствии норм законодательства, исключающих для ряда категорий работников судебный порядок рассмотрения индивидуальных трудовых споров, положениям Конституции СССР, законов СССР, международных актов о правах человека : заключение Комитета конституционного надзора СССР от 21.06.1990 № 2-2 // Ведомости СНД и ВС СССР. – 1990. – № 27. – Ст. 524.

освобождения от должности, перевода на другую работу и наложения дисциплинарных взысканий на должностных лиц, занимающих посты на высоком уровне, чьи функции согласно принятым международно-правовым нормам обычно рассматриваются как относящиеся к определению политики или к управлению, или носят строго конфиденциальный характер».

Сравнивая две процитированные нормы, можно констатировать, что в них идет апробация нового термина, который шире категории «секретный», ассоциируемой с государственной тайной.

Демократические преобразования, начавшиеся в нашей стране на последнем этапе существования СССР, с первых шагов убедительно доказали, что демонтаж системы, в которой гражданин был работником у единственного работодателя в лице государства, и оно же выступало в качестве своеобразного pater familias по отношению к материальным благам и даже к праву гражданина на индивидуальность и неприкосновенность частной жизни, будет иметь самые глубокие последствия, где одним из важнейших элементов выступает новая система взаимоотношений между государством и гражданином.

Принятие новой Конституции Российской Федерации, в тексте которой права и свободы человека и гражданина заняли, наконец, подобающее место, сформировало фундамент для *должного* в системе правового регулирования, делегировав реализацию *сущего* законодательным и подзаконным актам.

Исследователи отношений в области информации обычно начинают анализ конституционных норм со статей 23 и 24 текста Основного закона, определяющих систему защиты частной жизни граждан и сведений о ней. Авторский коллектив же хотел бы начать анализ конституционных положений с части первой статьи 45, которая устанавливает, что «государственная защита прав и свобод человека и гражданина в Российской Федерации гарантируется».

Как отмечают Ю. А. Дмитриев и Ю. И. Скуратов, «провозглашение в комментируемой статье Основного закона гарантируемой каждому человеку и гражданину государственной защиты его прав и свобод означает, с одной стороны, признание государством на самом высшем уровне своей обязанности защищать права и свободы, с другой стороны – наличие корреспондирующего к ней права человека и гражданина требовать от государства (его органов) выполнения взятой на себя обязанности»[1].

Отсюда следует, что государство обязано сформировать систему своих органов, которые должны обеспечивать такую защиту и наделить их

[1] Конституция Российской Федерации : доктринальный комментарий / под рук. Ю. А. Дмитриева, Ю. И. Скуратова. – М. : Статут, 2013. – С. 180.

соответствующими полномочиями. Одним из таких органов государства, имеющемся в подавляющем большинстве стран мира, является полиция (милиция), на которую возлагаются обязанности по защите жизни, здоровья, имущества, а в целом ряде случаев – жизни и достоинства граждан.

В современном мире, обладающем чрезвычайной динамикой в части коммуникативного общения и перемещения граждан, выполнение задач по обеспечению их защиты невозможно без накопления и обработки колоссального объема информации, среди которой в необходимый момент времени выделяются нужные сведения, на основании которых принимается соответствующее решение. При этом как граждане имеют право на защиту частной информации, так и некоторые государственные органы должны иметь легальный доступ к такой информации. Но, получив доступ и сами сведения, органы государства не могут сделать их общедоступными или иным образом произвольно с ними обращаться – они обязаны обеспечить к таким сведениям ограниченный доступ и исключить их распространение, которое без соответствующего административного разрешения считается противоправным.

СССР был весьма закрытым государством: на его карте не обозначались целые города, определенные районы маскировались под наименования других районов. Все это делалось для того, чтобы сохранить обороноспособность государства.

По данному поводу в свое время очень метко высказался В. А. Рубанов, одним из первых заявивший, что «действующая в стране система защиты секретов складывалась, как известно, в сложных исторических условиях. Она зародилась в трагический для советского народа период «обострения классовой борьбы», выкристаллизовалась в годы Великой Отечественной войны и укрепилась во времена войны «холодной». После косметического очищения на рубеже 50-60-х годов от наиболее одиозных и архаичных форм использования института государственной и военной тайны не по прямому назначению, а в ряде случаев и для прикрытия беззаконий система защиты секретов, хотя по-своему и совершенствовалась, но все более отставала от потребностей общественного прогресса»[1].

Во времена позднего СССР в аппарате государственного управления (таким образом именовалась в тот период нынешняя исполнительная власть) функционировало только два режима защиты документированной информации – режим секретности (режим защиты государственных секретов) и режим защиты служебных сведений, помечаемых как информация «Для служебного пользования». Ни о какой иной, в том числе

[1] Рубанов В. А. От «культа секретности» к информационной культуре // Коммунист. – 1988. – № 3.

конфиденциальной, информации речи не шло. И одной из важнейших задач стало отделение «государственно-значимой» информации (в понимании авторского коллектива, сведений об обороне, безопасности государства и иной внутрисистемной информации) от иных сведений, подлежащих защите при их попадании в органы государственной власти. Впоследствии такая информация получила системное название конфиденциальной в вышеуказанном законе об информации 1995 г.

Разделение этих систем между собой осуществлялось с большими трудностями, непоследовательно и до сего времени не нашло своего завершения. Поэтому без некоторого анализа основной для того времени системы защиты государственных секретов и трансформации ее в систему защиты государственной тайны общую картину данных отношений нарисовать не удастся.

Итак, к своему исчезновению с политических и географических карт мира СССР пришел с довольно стройной и логичной системой, именуемой «государственные секреты». Сущность ее заключалась в том, что категория «государственные секреты» делилась на две подкатегории – государственную и служебную тайну, которые, естественно, между собой пересекались.

Государственная тайна представляла собой верхний уровень системы и, начиная с 70-х годов XX в., стала ограничиваться перечнем главнейших сведений, составляющих государственную тайну, который утверждался секретным постановлением СМ СССР. Именно там концентрировались категории сведений, которые по мнению руководства страны необходимо было особым образом защищать. В основном они касались обороны и безопасности государства, сведения о правоохранительной деятельности затрагивали агентурно-оперативную работу. Для обозначения сведений, отнесенных к государственной тайне, использовались грифы секретности «Особой важности» и «Совершенно секретно».

Следует отметить, что уже в 70-е и последующие годы существовали серьезные ограничения на использование грифа секретности «Особой важности». Это было связано с двумя основными моментами: первый заключался в трудоемкости массового оформления самой жесткой формы допуска, связанного с весьма значительным объемом проверочных мероприятий; второй – с необходимостью осуществления большого комплекса технических мероприятий по защите информации по так называемым «побочным» каналам, на которые требовались весьма значительные финансовые ассигнования. Поэтому к сведениям с грифом «Особой важности» уже в тот период (и тем более в наше время) относился весьма небольшой массив сведений, носящих обобщенный характер, которые касались ключевых вопросов обороны и безопасности государства.

Сведения с грифом «Совершенно секретно» представляли собой более широкий класс информации, относимой к государственной тайне, и охватывали большой спектр защищаемой информации по категориям – здесь уже было место для правоохранительной деятельности. Так, в частности, к совершенно секретным относились обобщенные сведения о состоянии преступности в СССР, а также блок сведений, раскрывающих формы, методы оперативной работы и личность граждан, сотрудничающих с органами внутренних дел на конфиденциальной основе.

При этом реальный массив сведений со степенью секретности «Особой важности» и «Совершенно секретно» имел тенденцию к постепенному уменьшению. Самым же большим по объему был массив информации, имевшей гриф «Секретно», относимый уже к служебной тайне.

Объяснялось такое положение тем, что относимость сведений к служебной тайне осуществлялась на ведомственном уровне и любое министерство было вправе защищать в этом режиме практически любые сведения. В условиях острого идеологического и оборонного противостояния между СССР и блоком НАТО закрытость информации приветствовалась, поэтому деятельность большинства административных ведомств на союзном уровне осуществлялась, в основном, под покровом секретности.

Второй составляющей создавшегося положения было также нежелание партийного руководства нашего государства сообщать гражданам реальную информацию о состоянии экономики, социальной сферы, уровне преступности и многих иных важных для общества сведениях. Как отмечается в работе «Государственная тайна в Российской Федерации», в Советском Союзе «имела место административно-правовая система защиты государственных тайн. При этом существовало фактически две системы тайны: государственная и партийная. Традиционно существовавшие в нашей стране стереотипы примата власти над правом обуславливали долгие годы существовавшую политико-правовую ситуацию, когда секретность выступала в качестве социального института, возвышающегося над многими иными социальными институтами»[1].

При всех имевшихся недостатках политико-правового свойства созданная в СССР система обеспечения защиты государственно-значимой информации имела и очевидные достоинства. Одним из них являлась четкая линия на повышение степени секретности сведений по мере их обобщения. Например, в Перечне сведений, подлежащих засекречиванию в органах внутренних дел, утвержденном Приказом МООП СССР от

[1] Государственная тайна в Российской Федерации / под ред. М. А. Вуса. – СПб., 2000. – С. 21.

05.05.1968 № 0185, сведения в области мобилизационной работы и гражданской обороны на уровне края (области) имели степень секретности «Секретно», на уровне союзной республики – «Совершенно секретно», на уровне МООП СССР – «Особой важности».

Отсюда следует, что служебная тайна являлась административным институтом, в рамках которого осуществлялась первичная защита информации, по мере ее обобщения становившаяся государственной тайной.

Эта важнейшая роль института служебной тайны впоследствии была утрачена и до настоящего времени не восстановлена, что отрицательно сказывается на всей системе защиты государственной тайны, в особенности при современных методах и способах обработки и хранения информации.

Как отмечает А. А. Фатьянов, «водораздел между открытостью и закрытостью в деятельности органов государственной власти не во всех случаях должен проходить по границе между государственной тайной и общедоступной информацией – такой подход был бы слишком прямолинейным. Для иллюстрации данного утверждения рассмотрим небольшой пример. Выработка сколько-нибудь значимого управленческого решения, в особенности затрагивающего интересы многих лиц, всегда проходит в условиях столкновения позиций, рассмотрения значительного числа вариантов, оценки возможных последствий и т.п. Преждевременное распространение такой информации может излишне и необоснованно взбудоражить общественное мнение, подтолкнуть организации к скоропалительным решениям, изменить котировку акций – иными словами, внести дисбаланс в работу многих социальных и рыночных механизмов, обеспечивающих общественную стабильность»[1].

Следует отметить, что данная существенная функция служебной тайны для современного периода была важна и для советского времени – дозированное сообщение информации обеспечивало общественную стабильность. Правда, сообщение информации гражданам советского государства было излишне дозированным.

Правовая ситуация изменилась в связи с принятием в 1993 г. Закона Российской Федерации «О государственной тайне»[2], который установил системные признаки государственной тайны и определил, что сведения, составляющие государственную тайну, имеют степени секретности «Особой важности», «Совершенно секретно» и «Секретно». Таким образом, de facto была ликвидирована система государственных секретов и возник правовой вакуум в отношении института служебной тайны. Помимо ука-

---

[1] Фатьянов А. А. Правовое обеспечение безопасности информации в Российской Федерации – М., 2001. – С. 161.

[2] О государственной тайне : закон Российской Федерации от 21 июля 1993 г. № 5485-1 // СПС «Консультант Плюс».

занного, сложилась парадоксальная ситуация в отношении сведений, ранее отнесенных к служебной тайне и имевших гриф «Секретно». В их статус ни закон о государственной тайне, ни принятые в его развитие нормативные правовые акты никакой определенности не внесли, и они автоматически стали считаться государственной тайной. А ведь, как авторский коллектив показал выше, ранее эту информацию специально обособляли от государственной тайны, полагая ее менее значимой. В Инструкции по обеспечению режима секретности, утвержденной Постановлением СМ СССР от 12.05.1987 № 556-126, служебная тайна определялась как «охраняемые государством сведения в любой области науки, техники, производства и управления, разглашение (передача, утечка и т.п.) которых может нанести ущерб интересам государства».

В данной дефиниции необходимо обратить внимание на два ключевых слова: «любой» и «интерес». То есть речь идет о любой области государственной деятельности, в том числе, скажем, организации здравоохранения, образовании и т.п., где может возникнуть некий государственный интерес, который необходимо защищать. Учитывая общую увлеченность засекречиванием как эффективным способом защиты от «потенциального внешнего противника», можно только представить объем того массива информации, который скопился за несколько десятилетий советской власти под грифом «Секретно» и в 1993 г. вдруг стал государственной тайной. Но ценность этой информации осталась по-прежнему не слишком высокой, что вынуждено было признать Правительство Российской Федерации, принимая постановление от 04.091995 № 870[1]. Правила, установленные данным актом, и действующие до сего времени, устанавливают следующее: «К секретным сведениям следует относить все иные сведения (то есть не особой важности и не совершенно секретные. – Авт.) из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, разведывательной, контрразведывательной или оперативно-розыскной области деятельности».

В сравнении с определением советского периода предметная область для этой информации сужена, но во всем ином ее реальная значимость (ценность) стала еще более легковесной, так как субъектом интереса отныне стало не государство, а организация, то есть субъект однозначно локальный. И все это последствия одного не слишком продуманного законодательного решения.

[1] Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности : постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 // СПС «Консультант Плюс».

Последствия образовавшегося вокруг института служебной тайны правового вакуума не заставили себя долго ждать. Уже в 1994 году служебная тайна изумительным образом становится гражданско-правовым институтом путем включения данного понятия в текст части первой ГК РФ (ст. 139) и приобретает признаки, практически идентичные с коммерческой тайной. Комментаторы норм части первой ГК РФ в течение длительного времени воздерживались от каких-либо суждений относительно присутствия категории «служебная тайна» в ст. 139 ГК РФ, но в более близкий к современному период появились суждения следующего рода:

«Комментируемая статья практически не разделяет понятия служебной и коммерческой тайны, предусматривает одинаковое регулирование для обоих видов тайны, что связано с невозможностью четкого разделения регулируемых отношений. Информация, являющаяся коммерческой тайной, может стать служебной, и наоборот.

Состав информации, являющейся коммерческой и служебной тайной, также часто совпадает по составу с другими видами конфиденциальной информации, в том числе государственной, налоговой, банковской тайной. Так, согласно п. 2 ст. 102 Налогового кодекса Российской Федерации к разглашению налоговой тайны относится передача коммерческой тайны налогоплательщика. Большая часть информации, составляющей банковскую тайну, несомненно является коммерческой тайной для банка как коммерческой организации и служебной тайной для работников банка»[1].

В данном суждении, изобилующем доктринальными заблуждениями, на самом деле наиболее важным является то, что авторы признают обособленной служебную тайну от коммерческой тайны и пытаются выстроить какую-то логику перехода из одной системы ограничения в доступе к информации к другой.

Искусственность объединения служебной и коммерческой тайны была настолько очевидной, что законодатель, несмотря на наличие в тексте ГК РФ объединенной категории, принял Федеральный закон «О коммерческой тайне»[2], ни разу не упомянув в его тексте о служебной тайне.

Таким образом, правовая неопределенность в отношении института служебной тайны, который, по логике, должен являться основой для всей системы конфиденциальной информации в отечественном законодательстве, по-прежнему осталась.

Определенные сложности как в нормативном регулировании, так и в доктринальном осмыслении после разрушения советской системы законо-

---

[1] Комментарий к Гражданскому кодексу Российской Федерации (постатейный) / под редакцией Т. Е. Абоевой, А. Ю. Кабалкина : в 3 т. – Т. 1. – 3-е изд., перераб. и доп. – М. : Юрайт-Издат, 2007. – С. 166.

[2] О коммерческой тайне : федеральный закон от 29.07.2004 № 98-ФЗ // СПС «Консультант Плюс».

дательства постигли не только институт служебной тайны, но и другой, близкий к нему, институт служебной информации ограниченного распространения.

В советский период данный институт применялся в основном для исключения попадания определенных сведений в средства массовой информации. Интересное, но не бесспорное суждение по данному поводу высказывает Г. Г. Камалова:

«Особую часть сведений, не подлежащих оглашению и опубликованию, в советский период составляло содержание большого числа нормативно-правовых актов СССР. Хотя изначально в 1917 г. преобладала демократическая идея обнародования текстов нормативных документов, нашедшая свое отражение в декрете «О порядке утверждения и опубликования законов», согласно которому все нормативные документы после утверждения правительством подлежали публикации для всеобщего сведения и вступали в законную силу в день опубликования в официальной газете «Газета Временного Рабочего и Крестьянского Правительства», в последующие пять-шесть лет происходит отход от данного курса, и нормативные документы публикуются только с разрешения государственных органов различных уровней вплоть до 90-х гг. XX в.»[1].

Г. Г. Камалова правильно описывает одну из задач, которую решал институт сведений ограниченного распространения в советский период. Второй его задачей являлось исключение произвольного распространения сведений, которые не подпадали ни под какие перечни информации, подлежащей засекречиванию (отнесению к государственной или служебной тайне), но тем не менее огласка которых по мнению уполномоченных должностных лиц была нецелесообразной. В ряде случаев гриф «Для служебного пользования» проставлялся на изданиях в самых прозаических целях, например, чтобы обеспечить сохранность тиража от растаскивания.

Но постепенно, по мере избавления служащих советского государственного аппарата от мании тотального засекречивания, институт сведений ограниченного распространения нашел свое место в системе защиты информации – гриф (пометку) «Для служебного пользования» стали проставлять на документах сугубо служебного характера (например, планах расстановки сил милиции при проведении конкретного мероприятия с участием большого скопления людей).

Именно данная составляющая этого института и предопределила его «выживаемость» в новых общественно-политических условиях построения демократического государства, которая реализовалась в «Положении о порядке обращения со служебной информацией ограниченного распростра-

[1] Камалова Г. Г. Исторические особенности правовой охраны служебной информации ограниченного доступа (служебной тайны) в советский период // Вестник Удмуртского университета. – 2014. – Вып. 2. – С. 144.

нения в федеральных органах исполнительной власти», утвержденном Постановлением Правительства Российской Федерации от 03.11.1994 № 1233[1], правовой анализ которого авторский коллектив осуществит в следующем параграфе исследования.

Следующим этапом, на длительный по современным меркам период времени установившим определенную классификацию для систем ограничения в доступе к информации, стал Федеральный закон «Об информации, информатизации и защите информации»[2], ст. 10 которого установила, что «документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную».

Помимо указанного, данная статья федерального закона об информации, принятого в 1995 году, установила перечень информации, которую запрещено относить к информации ограниченного доступа, тем самым проведя законодательную черту между полностью общедоступной информацией и сведениями, в отношении которых возможно установление ограничений на доступ.

Подход законодателя при формулировании описанных правоположений представляет определенный научный интерес с точки зрения эволюции правового регулирования в рассматриваемой нами сфере общественных отношений, поэтому имеет смысл остановиться на них подробнее.

Первое, с чего начинает законодатель при установлении системы правоотношений, – это декларация о том, что государственные информационные ресурсы являются открытыми и общедоступными. Почему речь идет о декларации? Потому что при этом законодатель и намека не делает на то, чтобы установить административный механизм реализации свободного доступа к государственным информационным ресурсам. Без такого механизма описанное правоположение выглядит не более чем декларацией. Но даже в этой ситуации есть крупное рациональное зерно – с момента вступления в 1995 г. в силу федерального закона об информации при обращении граждан и организаций в органы государства, в распоряжении которых находятся те или иные государственные информационные ресурсы, последние стали обязаны обосновывать отказ в предоставлении сведений.

Далее следует указание на то, что документированная информация с ограниченным доступом представляет собой исключение из общего правила об открытости и общедоступности информационных ресурсов. Это бы-

---

[1] Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти : постановление Правительства Российской Федерации от 03.11.1994 № 1233 // СПС «Консультант Плюс».

[2] Об информации, информатизации и защите информации : федеральный закон от 20.02.1995 № 24-ФЗ // СПС «Консультант Плюс».

ло своего рода опровержение фактически сложившегося в советский период правила, согласно которому любая информация из органов государственной власти становилась открытой (общедоступной) только после разрешения соответствующих должностных лиц. Отныне вектор административных усилий должен был быть направлен на то, чтобы определять, какую информацию следует защищать (ограничивать к ней доступ), но не на то, чтобы разрешать распространение информации.

Закон об информации 1995 г. дал самое общее понятие конфиденциальной информации, обозначив ее как документированные сведения, доступ к которым ограничивается в соответствии с законодательством Российской Федерации. В данном определении ценным является только то, что ограничение на доступ к информации устанавливается именно законодательными нормами, но не нормами иных правовых актов, что предоставляло бы государственным органам излишнюю свободу в установлении ограничений на доступ к информации. Впрочем, в параграфе 1.2 настоящего исследования будет показано, что авторское толкование в данном случае не совпадает с судебным.

Далее закон об информации 1995 г. устанавливает интересную аналогию между административным механизмом отнесения сведений к государственной тайне и административным механизмом отнесения информации к категории конфиденциальной. Дело в том, что административно-правовой механизм отнесения сведений к государственной тайне довольно четко описан в законе о государственной тайне и законодатель при формулировании частей 4 и 5 ст. 10 закона об информации ясно намекает на то, чтобы взять его как модель при установлении аналогичных механизмов в законодательных актах, определяющих статус тех или иных видов конфиденциальной информации и основания для введения ограничений на доступ к ним.

Законодателя в данном случае легко понять, так как по состоянию на начало 1995 г. новая система ограничения в доступе к определенным категориям сведений находилась в стадии зарождения, было еще много неясного, поэтому законодатель двигался вперед очень осторожными шагами.

Но тем не менее в отношении одного вида конфиденциальной информации было допущено исключение. Речь идет об информации о гражданах (персональных данных). По мнению авторского коллектива, реальные позитивные подвижки в правовом регулировании защиты персональных данных и том внимании, которое государство и общество уделяют данной проблеме ныне, во многом является реализацией положений, изложенных в законе об информации 1995 г.

Между тем разрозненный массив категорий сведений, квалифицируемых как конфиденциальные, начал постепенно

наращиваться в законодательстве, возникла необходимость в его систематизации, которая был осуществлена путем установления указом Президента Российской Федерации перечня сведений конфиденциального характера[1]. Интересен также тот факт, что несмотря на наличие в законодательстве значительного массива норм, связанных с конфиденциальной информацией, далеко не вся она стала предметом данного перечня.

Для более полного раскрытия темы данного параграфа исследования целесообразно подвергнуть анализу содержательную часть перечня.

Первым пунктом в нем указаны «сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях».

События последующего времени показали, что личная тайна, объективированная в законодательстве как персональные данные, занимает в сложившейся системе нормативного правового регулирования данных отношений одно из самых ведущих мест и ее значимость продолжает повышаться. Это связано со многими социальными и политическими процессами, в том числе с осознанием необходимости неукоснительного исполнения норм Конституции Российской Федерации, связанных с защитой прав и свобод человека и гражданина.

Можно сказать, что институт персональных данных в рамках более значительного правового образования под названием «конфиденциальная информация» постепенно стал одним из самых фундаментальных и с ним прямо или косвенно связаны многие иные правовые системы ограничения в доступе к информации, ряд из которых (некоторые из профессиональных тайн) являются даже производными от института персональных данных.

Второй блок сведений, относимых в соответствии с рассматриваемым перечнем к категории конфиденциальных, образуют «Сведения, составляющие тайну следствия и судопроизводства». Необходимо сразу обратить внимание на тот факт, что речь в данном случае не может идти о единой категории – тайна следствия (правильно – тайна предварительного расследования[2], так как защита должна осуществляться не только в рамках проведения предварительного следствия, но и в рамках осуществления дознания как формы предварительного расследования) является институтом ограничения в доступе к любой информации, образовавшейся в процессе проведения

---

[1] Перечень сведений конфиденциального характера : указ Президента Российской Федерации от 06 марта 1997 г. № 188 // СПС «Консультант Плюс».

[2] Фатьянов А. А. Правовое обеспечение безопасности информации – М., 2001. – С. 273 и далее.

расследования, в том числе не имеющей статуса конфиденциальной. Второй институт, именуемый в перечне как тайна судопроизводства, правильно называется тайной совещания судей, так как никакой иной тайны судопроизводства в отечественном процессуальном праве быть не может – одним из существенных достижений современных цивилизованных правопорядков является гласность судебного разбирательства. Документированной информации конфиденциального характера при реализации норм о тайне совещания судей не образуется.

Третий блок сведений, включенных в перечень, образуют «сведения о лицах, в отношении которых в соответствии с федеральными законами от 20 апреля 1995 г. № 45-ФЗ "О государственной защите судей, должностных лиц правоохранительных и контролирующих органов" и от 20 августа 2004 г. № 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства", другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну»[1] и другими нормативными правовыми актами Российской Федерации».

Действительно, среди мер безопасности, которые могут применяться в отношении защищаемого лица, указано обеспечение конфиденциальности сведений о защищаемом лице. По мнению авторского коллектива, в данном случае понятие «конфиденциальность сведений» является в большей степени условным, так как меры безопасности применяются, как правило, в тех случаях, когда речь заходит о реальной угрозе жизни человека. Удержать сведения о мерах безопасности у большого числа субъектов (изменение места работы, жительства, внешности и т.п.) в рамках непонятного режима защиты вряд ли удастся. Здесь в ряде случаев необходимо защищать информацию на уровне государственной тайны.

Следующей категорией, включенной в перечень, являются «служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна)».

Авторский коллектив хотел бы сразу обратить внимание на тот факт, что ГК РФ, начиная с 1 января 2008 года, не регулирует отношения, связанные со служебной тайной в связи с утратой юридической силы (исключением из Кодекса) ст. 139, о содержании которой говорилось

[1] О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства : федеральный закон от 20.08.2004 № 119-ФЗ // СПС «Консультант Плюс».

выше. Очевидно, что п. 3 рассматриваемого перечня в связи с этим требует корректировки.

Анализ вышеприведенного правоположения также показывает, что в нем по сути дается определение категории «служебная тайна», где в качестве основных ее признаков приводятся:

- сущностный – сведения служебные, то есть относящиеся к деятельности соответствующего органа государственной власти;

- формальный – ограничение права на доступ (распространение) сведений нормами законодательных актов федерального уровня.

Как представляется авторскому коллективу, указанных признаков для обособления служебной тайны от других видов конфиденциальной информации недостаточно, в связи с чем в научной литературе появляются суждения типа «служебная тайна – это некоммерческая тайна ведомства, учреждения, аппарата управления предприятий и организаций, которая должна быть известна строго определенному кругу должностных лиц»[1].

Попробуем ответить на вопрос: в чем дискуссионность данного доктринального определения и каковы были бы правовые последствия его реализации в законодательстве и правоприменительной практике?

Первое – попытка определения какого-либо понятия через отрицание с научной точки зрения, как правило, некорректна. В приведенной цитате такое определение присутствует: служебная тайна – некоммерческая тайна. Если вспомнить, что у коммерческой тайны есть вполне четкие признаки, то получается, что служебная тайна – это любая информация, которую пожелают засекретить.

Второе – неопределенность круга субъектов, которые вправе ограничивать доступ к информации. Это и некие «ведомства», и учреждения (обратим внимание на то, что субъект предельно неопределенный, но цельный, то есть лицо), а также «аппарат управления предприятий и организаций» – категория еще более неопределенная, так как в организациях (предприятие, если оно фигурирует в качестве субъекта права, также является организацией) есть четко определенные законодательством для каждого вида организаций органы управления, а не некий аппарат. И не все органы управления юридическими лицами наделены полномочиями ограничивать доступ к тем или иным объемам информации. К тому же в организациях, напрямую не связанных с органами государственной власти, никакой иной конфиденциальной информации, кроме коммерческой тайны и персональных данных, быть не может, если, конечно, она не передана им органами государственной власти.

[1] Загородников С. Н., Максимов Д. А. Чужие тайны и их защита: нормативно-правовые аспекты // Российский следователь. – 2014. – № 3. – С. 44.

Теперь о правовых последствиях. Ч. 4 ст. 29 Конституции Российской Федерации устанавливает следующее:

«Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Перечень сведений, составляющих государственную тайну, определяется федеральным законом».

Данное положение Основного закона нашего государства определяет современный стандарт комплекса информационных свобод человека и гражданина, реализация которых имеет важнейшее значение в эпоху глобальных информационных связей и бурного развития информационных технологий.

Схема построения правового регулирования для реализации указанной нормы Конституции в достаточной мере прозрачна: позволено осуществлять оборот любой информации, за исключением сведений, которые включены в перечни, определенные федеральными законами.

Служебная тайна в нормативной трактовке рассматриваемого перечня, а тем более в доктринальной трактовке С. Н. Загородникова и Д. А. Максимова, в данную объективную схему не вписывается.

Указанное является весьма значимой правовой проблемой, разрешению которой отчасти посвящено данное исследование.

Еще одной категорией, включенной в Перечень, являются «сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее)». Несомненно то, что профессиональные тайны являются элементом общей системы конфиденциальной информации, как режима защиты. Дело в том, что по градации, введенной А.А. Фатьяновым[1], они относятся ко вторичным системам ограничения в доступе к информации, то есть к системам, в рамках которых не определяется, что именно должно ограничиваться в доступе. Говоря иначе, профессиональные тайны есть некий объем информации, которая определена нормативно, либо отнесена к категории конфиденциальной управомоченным субъектом и защищается лицом, выполняющим работы или оказывающим услуги в рамках определенной профессиональной деятельности. Как правило, в режиме профессиональной тайны (эти режимы для разных профессий по большому счету схожи между собой, поэтому вполне возможно говорить об обобщенном режиме профессиональной тайны) защищается либо личная тайна граждан, либо коммерческая тайна субъектов предпринимательской деятельности.

[1] Фатьянов А. А. Правовое обеспечение безопасности информации – М., 2001. – С. 48.

Следующей категорией, включенной в рассматриваемый перечень, являются «сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна)».

Сведения, составляющие коммерческую тайну, совершенно справедливо отнесены к категории сведений конфиденциального характера. В настоящее время эта правовая система ограничения в доступе к информации является одной из наиболее нормативно разработанных. Помимо целой системы норм, объединенных в главу 75 ГК РФ, регулированию отношений в данной сфере посвящен отдельный федеральный закон[1].

Можно сказать даже больше: коммерческая тайна, наряду с персональными данными, в общем массиве конфиденциальной информации занимает одно из самых значительных мест.

Следующей категорией, которая включена в рассматриваемый перечень, являются «сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них».

Это довольно маленький институт, имеющий своих обязанных субъектов и определенные временные рамки. Обязанных групп субъектов здесь две: первая – патентные поверенные, то есть лица, оказывающие услуги по оформлению документов на получение патентов, вторая – организации, входящие в систему Роспатента, в которых концентрируются вышеуказанные сведения. Перечень этих организаций определен приказом Роспатента от 03.07.1997 № 87 «О конфиденциальности сведений о сущности изобретений, полезных моделей, промышленных образцов»[2].

Временной отрезок защиты сведений: от начала оформления документов либо поступления их в организации Роспатента до принятия решения о выдаче патента либо окончательного решения об отказе в такой выдаче.

Последней категорией, которая включена в рассматриваемый перечень, являются «сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц». Представляется, что симбиоз информации получаемой в данном случае лицом, осуществляющим ее обработку, может охраняться как в режиме персональных данных, так и служебной, либо профессиональной тайн.

---

[1] О коммерческой тайне : федеральный закон от 29 июля 2004 г. // СПС «Консультант Плюс».

[2] О конфиденциальности сведений о сущности изобретений, полезных моделей, промышленных образцов : приказ Роспатента от 03 июля 1997 г. № 87 // СПС «Гарант-2015».

В качестве заключения к данному разделу исследования авторский коллектив хотел бы отметить следующее.

1. Категория «конфиденциальная информация», как показал авторский коллектив в данном параграфе исследования, стала применяться в отечественном юридическом лексиконе в последние годы существования СССР, а целостное нормативное звучание для обозначения обособленного класса сведений получила в Федеральном законе «Об информации, информатизации и защите информации».

2. В СССР, начиная с 70-х гг. XX в., была создана вполне соответствующая потребностям государственного аппарата система обеспечения защиты государственно значимой информации, получившая название «государственные секреты». Самую значительную по объему составную часть общего массива защищаемой информации в данной системе составляла служебная тайна, отнесение сведений к которой осуществлялось на уровне органов государственного управления (административных ведомств). Система государственных секретов выглядела сбалансированной по степени значимости охватываемых ею сведений, составляющих государственную и служебную тайны.

3. Закон Российской Федерации «О государственной тайне» обособил государственную тайну от всех иных видов информации, в том числе включил в ее систему сведения, ранее относившиеся к служебной тайне. Это привело к существенной неопределенности правового статуса служебной тайны, которая не устранена до сего времени.

4. Основным предназначением системы служебной тайны в настоящий период времени авторский коллектив исследования видит:

- защиту конфиденциальной информации, принадлежащей гражданам и организациям, при ее представлении в органы публичной власти;

- защиту информации, которая при большем уровне обобщения будет составлять государственную тайну.

5. Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 06.03.1997 № 188, не в полной мере отражает сущность и содержание сформированных в отечественном законодательстве правовых систем ограничения доступа к информации и требует корректировки. Авторским коллективом в данном параграфе исследования обосновано следующее изменение и дополнение в данный Перечень:

1) пункт 3 изложить в редакции:

«Сведения, свободное распространение которых либо неограниченный доступ к которым объективно препятствуют исполнению органами государственной власти возложенных задач и вытекающих из них функций (служебная тайна)».

§ 2. Современное состояние правового регулирования в отношении сведений конфиденциального характера на законодательном уровне

Проведенный анализ эволюции правового регулирования в сфере сведений конфиденциального характера показывает не только разноуровневость такого правового регулирования, а также разную степень значимости данной информации с точки зрения уровня ее защиты, но и их значительное многообразие. Поэтому в интересах проводимого исследования авторский коллектив хотел бы ограничить анализ современного правового регулирования этих отношений следующими видами конфиденциальной информации: служебная тайна, персональные данные, коммерческая тайна, конфиденциальная информация, образующаяся в рамках реализации задач по обеспечению государственной защиты. Авторскому коллективу представляется, что вышеперечисленные категории сведений являются наиболее значимыми для деятельности органов внутренних дел, связанной с получением и оборотом конфиденциальной информации.

Рассмотрение поставленного вопроса следует начать с ряда положений ныне действующего системообразующего для сферы информационных отношений законодательного акта – Федерального закона «Об информации, информационных технологиях и о защите информации»[1].

Нормы, описывающие основные положения по ограничению в доступе к информации, сконцентрированы в данном акте в статье 9. Согласно части первой данной статьи «ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства».

Перечисление оснований для ограничения в доступе к информации, то есть реализации основополагающего конституционного права каждого на свободу информации, только на первый взгляд кажется всеобъемлющим. На самом деле здесь упущено одно из самых главных оснований – соблюдение прав и свобод самого гражданина, а не неких «других лиц». Авторскому коллективу это представляется упущением со стороны законодателя, которое следует исправить.

Часть вторая рассматриваемой статьи устанавливает, что «обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами».

На первый взгляд данная норма кажется основательной: ограничение прав и свобод граждан по Конституции Российской Федерации возможно только на основании федеральных законов, что распространимо и на систему

[1] Об информации, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 21.07.2014) // СПС «Консультант Плюс».

конфиденциальной информации. Однако попытаемся более системно взглянуть на ее содержание. По форме изложения это разрешение (правомочие) не полагает обязательным соблюдение положений подзаконных актов, регулирующих ограничения на доступ к информации. На основании ч. 2 ст. 9 закона об информации 2006 года, в частности, допустимо неисполнение Положения, утвержденного Постановлением Правительства Российской Федерации от 03.11.1994 № 1233 в связи с тем, что статус служебной информации ограниченного распространения не определен федеральным законом.

На основании указанного можно констатировать, что положения ч. 2 ст. 9 закона об информации правильны по сути, но ошибочны по изложению и могут привести к ошибкам в правоприменении.

В положениях ст. 9 содержится демонтаж системы информации ограниченного доступа, созданной законом об информации 1995 года. В частности, устанавливается, что защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством о государственной тайне. Обычно категория «законодательство» применяется в тех случаях, когда речь заходит о нескольких законах, регулирующих определенный блок общественных отношений. Например, вполне допустимо говорить о гражданском законодательстве и т.д. Но в сфере государственной тайны действует только один специальный законодательный акт – закон о государственной тайне, который, кстати, регулирует отношения в большей степени связанные не с защитой государственной тайны, а с порядком отнесения сведений к данной категории информации и установлением административных процедур засекречивания и рассекречивания.

Помимо указанного, следует отметить, что отношения, связанные с государственной тайной, прямо или опосредованно регулируются многими федеральными законами, в том числе и Федеральным законом «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию»[1], Уголовным кодексом Российской Федерации, Уголовно-процессуальным кодексом Российской Федерации, рассматриваемым нами Законом об информации 2006 года и т.д. Но ведь это не означает, что они в совокупности образуют законодательство о государственной тайне.

Далее, в ч. 4 ст. 9 предусматривается, что «федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую, служебную или иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение».

Совокупный анализ положений частей 2, 3 и 4 ст. 9 рассматриваемого закона об информации показывает, что категория «конфиденциальность» стала системным термином, синонимом категории «ограничение в

[1] О порядке выезда из Российской Федерации и въезда в Российскую Федерацию : федеральный закон от 15.08.1996 № 114-ФЗ // СПС «Консультант Плюс».

доступе к информации». Тем самым без каких-либо научных оснований на нормативном уровне ликвидирована удачная классификация закона об информации 1995 года, породившая целый класс специфичной конфиденциальной информации, отличной по уровню оборота и защиты от государственной тайны. По мнению авторского коллектива, такую классификацию следует восстановить.

В существенной мере «размыт» и блок системообразующих норм, связанных с персональными данными. Во-первых, в формулировках норм вообще не используется термин «конфиденциальность» и неясно, полагает ли закон об информации 2006 года сведения о частной жизни граждан конфиденциальными (то есть ограниченными в доступе). В ч. 8 ст. 9 лишь запрещается требовать от гражданина предоставления такой информации и получения ее помимо его воли, если иное не предусмотрено федеральными законами. Часть 9 ст. 9 устанавливает, что «порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных». Тем самым предопределяется содержание данного законодательного акта, хотя основное для него, по мнению авторского коллектива, заключается в установлении системы оборота персональных данных и системы контроля за соблюдением правил этого оборота.

На основании указанного авторский коллектив делает вывод о том, что категория «конфиденциальная информация» на системном законодательном уровне в настоящее время не воспринимается как некая совокупность групп сведений, имеющих ряд общих признаков, основными из которых должны являться уровень правового регулирования данных отношений и уровень их правовой защиты, хотя во многих нормативных правовых актах она по-прежнему выделяется в данном качестве.

Конфиденциальность информации теперь трактуется законом об информации 2006 года как правовая обязанность не передавать такие сведения третьим лицам без согласия ее обладателя (п. 7 ст. 2). Вот только как быть правоприменителю, если он не в состоянии испросить согласия обладателя информации, данный законодательный акт не определяет, как, впрочем, не определяет и многих иных важных положений относительно конфиденциальной информации.

В соответствии с основной задачей, определенной авторским коллективом для данного параграфа исследования, проведем анализ законодательного регулирования отдельных правовых систем ограничения в доступе к информации. Начнем со служебной тайны. Упоминание о данной системе как об обособленной имеется в двух нормах закона об информации 2006 г. Причем в первой из них (п. 3 ч. 4 ст. 8) служебная тайна поставлена в один ряд с государственной тайной. Речь идет о запрете на ограничение доступа к информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств,

если эти сведения на составляют государственную или служебную тайну. Тем самым признается, что институт служебной тайны является одним из двух институтов ограничения в доступе к информации в органах публичной власти. Однако эта важнейшая для обеспечения информационной безопасности нашего государства и защиты прав граждан задача до сего времени на системном уровне не реализована.

При этом в близко по тексту расположенной норме (ч. 4 ст. 9) законодатель упоминает служебную тайну в контексте с коммерческой тайной. Правда, в данном случае речь идет о том, что на законодательном уровне должны устанавливаться условия отнесения информации к служебной тайне.

Раскроем несколько более подробно смысл данного положения. Отнесение сведений к государственной тайне строится на основе двух перечней: перечня сведений, составляющих государственную тайну, и перечня сведений, которые не могут составлять государственную тайну. По отношению к коммерческой тайне, в один ряд с которой в ст. 9 поставлена и служебная тайна, такой подход неприменим из-за многообразия субъектов и отношений. Поэтому законодатель в ГК РФ и Законе о коммерческой тайне определяет только совокупность признаков, при наличии которых обладатель информации вправе распространить на нее режим коммерческой тайны. Такая же схема предлагается и в отношении служебной тайны и она, в принципе, является приемлемой.

Добавим к вышесказанному, что служебная тайна как категория отражена в нормах еще более чем пятидесяти федеральных законов, где она определяется как самостоятельный институт и поставлена в один ряд с государственной и коммерческой тайной, то есть институтами, основные регулятивные нормы которых сконцентрированы в специальных законах. По отношению к служебной тайне в этом также есть настоятельная необходимость.

Пока же констатируем, что de facto институт служебной тайны в настоящее время чаще всего ассоциируется с институтом сведений ограниченного распространения в федеральных органах исполнительной власти, что отчасти справедливо по следующим соображениям. Во-первых, после более чем двадцатилетнего перерыва возвращение системы государственных секретов вряд ли целесообразно. Таким образом, гриф «Секретно» прочно связан с государственной тайной и там сформировалась единая ступенчатая система защиты. Во-вторых, гриф «Для служебного пользования» до сих пор применяется при довольно скупом правовом регулировании, он привычен и распространен. Надо лишь придать современное звучание всей этой системе, поднять регулирование до уровня федерального закона, описать систему отнесения сведений к служебной тайне и режим защиты служебной тайны – получится вполне корректный институт.

Однако в настоящее время данная система обладает целым рядом существенных недостатков, на которых следует акцентировать внимание. Так, необходимо подвергнуть выборочному анализу нормы «Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии», утвержденного Постановлением Правительства Российской Федерации от 03.11.1994 № 1233.

При анализе любой правовой системы ограничения в доступе к информации наиболее существенными элементами данной системы, на которые следует обратить внимание, являются: а) определение того, какую именно информацию мы собираемся относить; б) перечень информации, ограничивать доступ к которой запрещается; в) кто уполномочен ограничивать доступ и снимать ограничения; г) максимальный срок действия ограничений.

Именно под данным углом зрения авторский коллектив и проведет анализ. Итак, в соответствии с п. 1.2 положения к служебной информации ограниченного распространения относится «несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью».

Данная дефиниция порождает целый ряд вопросов, первым из которых является: а что такое несекретная информация? Понятие «секретная информация» является скорее сленговым, чем официальным и, по мнению авторского коллектива, означает информацию, отнесенную к государственной тайне. Видимо, так следует и указать, тем более в п. 1.1 рассматриваемого акта прямо устанавливается, что «положение не распространяется на порядок обращения с документами, содержащими государственную тайну».

Далее, о каких организациях в рассматриваемом определении идет речь, если прежде всего положение регулирует обращение с информацией в органах государственной власти. Формально-логически любой орган государственной власти есть организация, но это организация с особым статусом, поэтому заслуживает отдельного упоминания.

И последний, наверное самый важный момент: единственным системным признаком, отличающим информацию ограниченного распространения от любой иной информации, является признак служебной необходимости.

По данному поводу довольно объективное суждение высказывает Ю. И. Павлов, который отмечает, что «поскольку критерием отнесения тех или иных сведений к категории служебной информации ограниченного распространения являются не конкретные объективные факторы, а субъек-

тивная категория – “служебная необходимость”, возникает повод для возможности принятия произвольных правоприменительных решений»[1].

По мнению авторского коллектива настоящего исследования, речь идет не просто о поводе, а об объективной возможности прямого произвола по отношению к распространению информации. Обратим внимание на тот факт, что в рассматриваемой дефиниции речь идет не о служебной информации, которую хоть как-то возможно выделить из общего информационного массива, а о любых сведениях, распространение которых можно ограничить, если возникает так называемая служебная необходимость.

Заметим также, что закон об информации 2006 г. устранил в данном вопросе малейшие неопределенности (хотя таковых, по мнению авторского коллектива настоящего исследования, не было и в законе об информации 1995 г.), конкретно установив, что «ограничение доступа к информации устанавливается федеральными законами» (ч. 1 ст. 9), но это ни коим образом не изменило статуса положения о порядке обращения со служебной информацией ограниченного распространения, хотя указанная норма федерального закона действует уже около десяти лет.

Хотя правильным, вытекающим из норм действующего законодательства, является принятие отдельного федерального закона, регулирующего оборот данного вида информации, авторский коллектив тем не менее предлагает внести некоторые уточнения в определение служебной информации ограниченного распространения, изложив п. 1.2 положения в следующей редакции:

«К служебной информации ограниченного распространения относятся сведения конфиденциального характера, касающиеся деятельности федеральных органов государственной власти и подчиненных им организаций, свободное распространение которых создает препятствия для исполнения указанными органами и организациями установленных для них задач и функций».

Обратимся к анализу следующей нормы, определяющей перечень сведений, которые не могут быть отнесены к служебной информации ограниченного распространения.

Первую категорию, включенную в данный перечень, составляют «акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации».

Данное положение по своей правовой сущности является пересказом ряда конституционных норм, за исключением не применяемой в тексте Конституции Российской Федерации категории «акты законодательства». Неопределенность данной категории является почвой для «вольных» трак-

[1] Павлов И. Ю. Современные проблемы правового регулирования государственной и служебной тайны в России // Ленинградский юридический журнал. – 2013. – С. 35.

товок типа приведенной выше правовой позиции Верховного Суда Российской Федерации. Поэтому она должна быть заменена на категорию «нормативные правовые акты», имеющую большую доктринальную определенность и официально употребляемую в законодательстве для совокупного обозначения законодательных и подзаконных нормативных актов.

Во всем остальном недопустимость ограничения в доступе к указанным актам следует признать обоснованной.

Следующей категорией, включенной в перечень, являются «сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация, необходимая для обеспечения безопасного существования населенных пунктов, граждан и населения в целом, а также производственных объектов».

Проблема открытости перечисленных видов информации – это прежде всего проблема ответственности органов публичной власти перед населением в случаях реального возникновения или угрозы возникновения чрезвычайных ситуаций природного либо техногенного характера. К сожалению, в советский период были случаи сокрытия крупных аварий, в том числе имевших пролонгированные опасные последствия. Данное обстоятельство и послужило причиной установления этого ограничения. Аналогичное правоположение содержится и в Законе о государственной тайне.

Следующим блоком информации, доступ к которой не может быть ограничен, является «описание структуры органа исполнительной власти, его функций, направлений и форм его деятельности, а также его адрес».

Истоки данного положения следует искать в Конституции Российской Федерации. Как установлено в ее ст. 15, «любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы для всеобщего сведения».

Любой орган исполнительной власти задействован в системе исполнения законодательных предписаний, поэтому так или иначе взаимодействует с гражданами, формируя для какой-то части из них обязательные предписания, осуществляя контроль и надзор и т.д. Задачи и функции каждого органа исполнительной власти определяются нормативным правовым актом. Следовательно, граждане вправе знать статус, задачи и функции любого органа исполнительной власти, что и отражено в рассматриваемой норме.

Еще одним блоком информации, на доступ (распространение) которой не могут быть наложены ограничения, является «порядок рассмотрения и разрешения заявлений, а также обращений граждан и юридических лиц».

Данная информация в общем и целом никогда не являлась закрытой, однако категорию «порядок рассмотрения» в данном конкретном случае можно истолковывать двояко: а) как общую процедуру; б) как путь конкретного обращения гражданина по подразделениям административного ведомства. При истолковании данной нормы в этом контексте она представляет собой значительную ценность.

Следующим блоком информации, на доступ (распространение) которой не могут быть наложены ограничения, являются «решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке». При всей очевидности общедоступности такого рода сведений разработчики рассматриваемого акта совсем не случайно включили данный пункт в перечень, так как благодаря бюрократическим уловкам такая информация может быть доступна для конкретного заявителя, но не являться в целом общедоступной.

Следующим блоком информации, на доступ (распространение) которой не могут быть наложены ограничения, являются «сведения об исполнении бюджета и использовании других государственных ресурсов, о состоянии экономики и потребностей населения».

Данный пункт выглядит скорее декларативным, чем реальным. Среди сведений об исполнении бюджета и использовании различных государственных ресурсов имеется законное место для закрытой информации, в том числе и для сведений, составляющих государственную тайну. Чтобы преодолеть в данном случае противодействие должностных лиц, препятствующих распространению информации такого рода, необходимо более точно определить признаки информации, доступ к которой не может быть ограничен.

Сведения о состоянии экономики и потребностях населения являются в Российской Федерации полностью открытыми уже значительное время.

Последним из блоков сведений, на доступ (распространение) которых не могут быть наложены ограничения, являются «документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах организаций, необходимые для реализации прав, свобод и обязанностей граждан».

Данная норма сформулирована таким образом, что в открытые фонды библиотек возможно ограничивать доступ в тех случаях, когда он не обоснован задачами реализации прав, свобод и обязанностей граждан. Не проще ли просто признать открытые информационные ресурсы полностью общедоступными?

Общий административный механизм упорядочения оборота и защиты служебной информации ограниченного распространения имеет несколько составляющих. Первый компонент заключается в том, что руководитель федерального органа исполнительной власти определяет категории

должностных лиц, уполномоченных относить данные сведения к разряду ограниченного распространения. В зависимости от политики административного ведомства в части открытости перед обществом этот перечень может быть узким и широким. Например, в Минобороны России число должностных лиц, принимающих такие решения, объективно должно быть больше, чем в Минсельхозе России и тем более чем в Минкультуры России.

Второй компонент – установление руководителем административного ведомства порядка передачи служебной информации ограниченного распространения другим органам и организациям. По мнению авторского коллектива настоящего исследования, данный порядок должен быть унифицированным и определяться централизованно, но не быть различным от ведомства к ведомству, так как это может создать почву для различных злоупотреблений.

Третий компонент – установление руководителем административного ведомства порядка снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения.

Снятие пометки есть по сути снятие ограничений на распространение сведений. Это очень важное мероприятие, которое связано с обеспечением конституционных прав и свобод человека и гражданина в информационной сфере. Оно имеет три составные части:

- установление порядка снятия ограничений по миновании надобности;
- установление порядка снятия ограничений по истечении предельного срока на их введение;
- установление порядка снятия ограничений в связи с необходимостью раскрытия информации.

Ни одна из этих очевидных для данной области общественных отношений административных процедур в положении не описана, хотя столь же очевидным является то, что данные процедуры не могут быть различными от одного административного ведомства к другому.

Заинтересованные лица вправе знать, каким образом и когда они могут получить доступ к определенной скрываемой от них информации.

Четвертый компонент – организация защиты служебной информации ограниченного распространения. Некоторые элементы системы защиты описаны в разделе положения «Порядок обращения с документами, содержащими служебную информацию ограниченного распространения». Авторский коллектив подвергнет его анализу чуть ниже, здесь же отметим, что правильным было бы возложить на руководителей административных ведомств не определение организации защиты этой информации, а определение особенностей защиты, если таковые имеются. Общая же система защиты должна быть определена централизованно.

В п. 1.6 положения устанавливается, что «должностные лица, принявшие решение об отнесении служебной информации к разряду ограни-

ченного распространения, несут персональную ответственность за обоснованность принятого решения и за соблюдение ограничений, предусмотренных п. 1.3 (перечень сведений, в отношении которых введение ограничений не допускается. – Авт.) настоящего положения».

Установление персональной ответственности за принятие решения об установлении ограничений на распространение информации является важным элементом для упорядочения отношений в данной сфере. Однако здесь есть два момента. Первый из них – персональная ответственность во всех случаях индивидуализована по субъекту, то есть решение путем волеизъявления принимает конкретное должностное лицо, оно же и несет бремя ответственности за принятое решение. А как быть в случае, если данный гражданин после принятия решения переведен на другую должность либо вовсе прекратил свой служебный контракт? В данном случае бремя ответственности ложится на правопреемника и он, по логике, должен подвергать ревизии решения своего предшественника. Однако этот момент никак не урегулирован.

Второй момент – персональная ответственность во всех случаях должна иметь в потенции санкцию за нарушение нормативного предписания. Причем только дисциплинарной ответственностью здесь не обойтись, так как необоснованное установление ограничений на доступ к информации в современных условиях повышения степени открытости публичной власти перед обществом и стремительной информатизации должно образовывать как минимум административное правонарушение.

Пункт 1.7 Положения устанавливает, что «служебная информация ограниченного распространения без санкции соответствующего должностного лица не подлежит распространению (разглашению)». Как представляется авторскому коллективу, в данном случае целесообразно внести большую конкретику в данную административную процедуру, а именно установить, что решение о снятии ограничений на распространение сведений ранее предельного срока, установленного при введении таких ограничений, либо общего предельного срока (об этом чуть ниже) принимается лицом, установившим ограничения, его правопреемником либо вышестоящим руководителем.

Теперь о сроках ограничений. Данная проблема имеет не только конкретно-прикладное, но и важное общепрактическое значение. Конкретно-прикладное заключается в том, что уполномоченное должностное лицо при принятии решения об ограничении на распространение информации сразу же устанавливает предельный срок, по истечении которого сведения переходят в разряд общедоступных. Такой подход снимает целый ряд вопросов.

Помимо указанного, необходимо нормативно, как минимум на уровне данного положения, а как максимум – на уровне федерального за-

кона определить общий предельный срок установления ограничений на распространение информации в данном режиме. Это важно не только для реализации задач обеспечения доступа, но и для того, чтобы минимизировать негативные последствия от введения ограничений путем повышения ответственности должностных лиц за принимаемые решения, так как в данном случае противоправные решения через определенный срок станут достоянием общественности.

Теперь подвергнем краткому анализу правовое регулирование оборота служебной информации ограниченного распространения, установленное рассматриваемым положением. Первое, на что следует обратить внимание, это полное ориентирование регулятивных норм на оборот исключительно документов на бумажных носителях. Второе – бремя юридической ответственности за обоснованность простановки на документе пометки «Для служебного пользования» возлагается положением одновременно на исполнителя документа и лицо, подписавшее документ, что, по мнению авторского коллектива, является неправильным. Исполнитель, подготовивший документ, всего лишь высказывает свое предположение о его содержании. Юридически значимое решение принимает лицо, подписавшее данный документ, оно и должно нести ответственность за неправомерность простановки вышеуказанной пометки.

Учет документов с пометкой «Для служебного пользования» осуществляется в подразделениях так называемого «общего» делопроизводства, что подчеркивает второстепенность статуса данной системы как меры реального ограничения в доступе к определенным объемам информации.

Третье – за обеспечение сохранности данной категории документов устанавливается персональная ответственность, выражающаяся в том, что они передаются из подразделений делопроизводства работникам исполняющих подразделений под расписку. При этом, к сожалению, не устанавливается обязательность передачи данного документа под расписку от одного исполнителя другому, как это предусмотрено в отношении документов, содержащих сведения, составляющие государственную тайну. Правда, при этом устанавливается, что передача документов и дел с пометкой «Для служебного пользования» от одного работника другому осуществляется с разрешения соответствующего руководителя.

Двойственность статуса документов с пометкой «Для служебного пользования» подчеркивается еще и тем, что они, с одной стороны, размножаются (тиражируются) только с письменного разрешения соответствующего руководителя и хранятся в надежно запираемых и опечатываемых шкафах, а с другой стороны, допускается их пересылка в другие организации заказными и ценными почтовыми отправлениями, что, конечно,

повышает уровень их сохранности, но не настолько, чтобы исключить несанкционированное ознакомление с содержанием таких документов.

О фактах утраты документов, дел и изданий, содержащих служебную информацию ограниченного распространения, либо разглашения этой информации ставится в известность руководитель организации и назначается комиссия для расследования обстоятельств утраты или разглашения. Результаты расследования докладываются руководителю, назначившему комиссию.

Проведение служебного расследования по факту утраты или разглашения является важной мерой для упорядочения оборота данных сведений, однако при такой слабой организации учета фактов ознакомления практически невозможно защитить информацию от несанкционированного доступа к ней и противоправного копирования.

Поэтому можно однозначно констатировать, что при существующем уровне правового регулирования рассматриваемая система ограничения в доступе к информации малопригодна для организации реальной защиты сведений конфиденциального характера, поступающих в органы публичной власти. К тому же действие рассматриваемого положения распространяется только на федеральные органы исполнительной власти. Органы других ветвей государственной власти (судебной и законодательной) формально не имеют даже данного режима. Тем более его не имеют органы государственной власти субъектов Российской Федерации и органов местного самоуправления.

Отсюда следует, что целесообразно вновь вернуться к категории «служебная тайна» на общесистемном уровне, для чего поднять планку правового регулирования данных отношений до федерального закона, разработать единые унифицированные правила оборота таких сведений как на бумажных носителях, так и в электронной форме отображения, определив при этом, что любые сведения конфиденциального характера, к которым правомерно ограничен доступ их первичным обладателем и которые в рамках установленной процедуры переданы в органы публичной власти, должны сохраняться там в указанном режиме в течение срока, установленного законом либо согласованного сторонами соответствующих отношений.

Основными блоками отношений, связанных со служебной тайной, которые должны быть урегулированы на уровне федерального закона, авторскому коллективу представляются следующие:

1) установление общего статуса служебной тайны, то есть какие органы публичной власти вправе формировать перечни таких сведений, каким образом они экспертируются и в какие сроки подлежат пересмотру;

2) какие сведения недопустимо относить к служебной тайне;

3) порядок отнесения сведений к служебной тайне (кто вводит ограничения для конкретных блоков информации и на какой срок; кто может

принять решение о досрочном снятии ограничений; общий порядок снятия ограничений; особенности установления ограничений на доступ к информации в электронной форме отображения и т.д.);

4) основные положения, определяющие порядок оборота сведений, составляющих служебную тайну, внутри организации и порядок направления в другие организации, учет фактов ознакомления с отдельными категориями сведений (по мнению авторского коллектива, это коммерческая тайна и персональные данные, поступившие извне);

5) предельные сроки введения ограничений на доступ к сведениям, защищаемым в режиме служебной тайны.

Следующим блоком сведений конфиденциального характера, который требует анализа в рамках настоящего исследования, являются персональные данные. Категория «персональные данные» и основные контуры правового регулирования этой правовой системы ограничения в доступе к информации были установлены законом об информации 1995 г. Именно этот акт дал первое из легальных определений данной категории, установив, что «информация о гражданах (персональные данные) – (это) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность».

С доктринальной точки зрения очень важным является вопрос, соотносится ли категория «персональные данные» с категорией «частная жизнь» и каково это соотношение. В. В. Погуляев и Е. А. Моргунова полагают данные категории тождественными[1]. Авторскому коллективу настоящего исследования данное соотношение видится более сложным. Дело в том, что пределы своей частной жизни (условный барьер, за который недопустимо переходить) гражданин определяет для себя самостоятельно. В этом основная сложность в установлении объема информации, подлежащей защите. Например, многие представители артистической среды склонны к более широкому распространению информации о своей личной жизни, чем так называемые рядовые граждане. Это связано с необходимостью поддержки определенного уровня популярности.

Говоря о фундаменте при построении системы правового регулирования данных отношений, следует отметить, что они строятся на попытке некоторой формализации сведений, охватываемых категорией «частная жизнь» применительно к морально-нравственным устоям и традициям определенного общества.

Обратимся к действующей системе правового регулирования. Основным законодательным актом, который в настоящее время регулирует рассматриваемую совокупность общественных отношений, является Феде-

[1] Погуляев В. В., Моругина Е. А. Комментарий к Федеральному закону «Об информации, информатизации и защите информации» – М., 2004. – С. 132.

ральный закон «О персональных данных»[1]. В целях выполнения задач, поставленных авторским коллективом для настоящего исследования, данный акт будет подвергаться анализу под углом зрения проблем накопления и оборота этих сведений в органах публичной власти. Однако прежде необходимо более четко определиться с самим понятием «персональные данные». Первое легальное определение данной категории, приведенное в законе об информации 1995 г., было следующим: «Информация о гражданах (персональные данные) – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность».

Основной смысл, который вкладывал законодатель в данное определение, – к персональным данным относится информация, на основании которой мы можем сказать, что данное физическое лицо является гражданином таким-то. Юридическая формула «сведения о фактах, событиях и обстоятельствах жизни гражданина» представляется авторскому коллективу достаточно емкой и адекватной предмету этой информации.

В трактовке закона о персональных данных под эту категорию подпадает «любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация».

В данном определении мы видим две больших группы сведений. Первая из них связана с тем, что есть конкретный гражданин, он известен и индивидуально определен. К его персональным данным относится дополнительно получаемая о нем информация, помимо той, которая потребовалась для его индивидуального определения (идентификации). Скажем, есть Петров Сергей Иванович, родившийся 07.07.1980 в г. Воронеже, проживающий на улице Лизюкова, д. 1, кв. 11. Этих сведений вполне достаточно, чтобы полностью индивидуально определить конкретное физическое лицо, так как вероятность того, что имеется субъект с полностью совпадающими идентификационными данными, практически равна нулю.

Вторая группа сведений связана с тем, что осуществляется попытка по определенным системным признакам выявить конкретных лиц, которые подпадают под эти характеристики. Например, получение индентифицирующей информации в отношении лиц, которые имеют в определенном банке вклады на сумму свыше одного миллиона рублей, либо таких же данных на всех лиц, имеющих зарегистрированное огнестрельное оружие и проживающих в определенном населенном пункте.

Все было бы четко, если бы не нюанс, который превращает данную ситуацию в полную неопределенность, а именно: персональные данные –

[1] О персональных данных : федеральный закон от 27 июля 2006 г. № 152-ФЗ // СПС «Консультант Плюс».

это любая информация. Признание факта о том, что любая информация о физическом лице есть его персональные данные не может позволить выстроить приемлемую систему правового регулирования в силу изначальной неопределенности объекта правового регулирования.

Иными словами, если мы толком не знаем, что такое персональные данные, как мы можем выстроить систему ограничения доступа к этой информации? Например, является ли персональными данными информация о том, что упомянутый выше Петров Сергей Иванович имеет размер одежды 54, а размер обуви – 43? Формально это персональные данные (любая информация о лице), но нужно ли их защищать?

Выглядит странным допущение такой неопределенности при довольно четко определенной цели рассматриваемого федерального закона: обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Комплекс прав и свобод человека и гражданина в конечном итоге определен Конституцией Российской Федерации, поэтому в принципе возможно (хотя в ряде случаев это представляет собой довольно сложную научную задачу) связать любое конкретное конституционно-определенное право человека с информацией о конкретной личности, которую следует подвергать защите.

Обратим внимание на один существенный момент, имеющий значение для определения уровня правовой значимости прав и свобод в Конституции нашего государства. На первом месте (статья 19) стоит равенство всех перед законом и судом, на втором (статья 20) – право на жизнь, а на третьем (статья 21) – право на достоинство личности, которое охраняется государством, а уже затем следуют свобода, неприкосновенность частной жизни, защита чести и доброго имени и т.д.

Как представляется авторскому коллективу, система защиты персональных данных должна быть направлена на защиту жизни и достоинства личности, а затем уже не неприкосновенность частной жизни.

Категории «жизнь» и «частная жизнь» являются довольно общеупотребительными и в подробном анализе в рамках данного исследования не нуждаются. А вот на категории «достоинство» авторский коллектив хотел бы несколько более детально остановиться, так как мнения по данному поводу в научной среде не единодушны.

По мнению В. И. Червонюка, «достоинство личности – свойство человека, характеризующее его духовный облик и предполагающее отношение к нему со стороны государства, иных лиц как к высшей ценности»[1].

На сайте МВД Республики Адыгея (www.01.мвд.рф) приведено несколько иное суждение:

[1] Червонюк В. И. Конституционное право России : учебное пособие – М., 2004. – С. 56.

«Достоинство личности рассматривается с двух сторон. С одной стороны, достоинство личности – один из важнейших конституционных принципов, положенный в основу правового статуса личности, а также регулирующий взаимоотношения человека и государства. С этой позиции закрепление за человеком прав и свобод и их реализация являются проявлением достоинства личности.

С другой стороны, достоинство личности является самостоятельным субъективным правом человека. Достоинство личности предполагает определенную оценку со стороны общества и самооценку своих моральных и интеллектуальных качеств».

По мнению авторского коллектива, помимо вышеуказанных важных суждений, необходимо отметить, что достоинство личности есть обязанность должностных лиц государства и граждан соблюдать по отношению к любому человеку общепринятый в данном государстве и обществе стандарт отношения, позволяющий человеку чувствовать себя равным членом общества, претендующим на уважение со стороны представителей государства и других граждан.

Одним из проявлений реализации достоинства личности является предоставление гражданину субъективного права распространять положительно характеризующую его информацию (успехи) и скрывать отрицательно характеризующую (неуспехи). Институт персональных данных должен стоять на страже реализации данного субъективного права.

Одной из центральных категорий во всей системе законодательного регулирования отношений, связанных с персональными данными, является категория «оператор», под которой понимается «государственный или, муниципальный орган, юридическое или физического лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели их обработки, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными».

Юридический статус оператора персональных данных, как следует из контекста норм федерального закона о персональных данных, приобретается лицом автоматически с того момента, как оно начало обработку персональных данных. Соответственно, с этого момента на данное лицо возлагается комплекс обязанностей, предусмотренных нормами закона о персональных данных. Из данного определения со всей очевидностью также следует, что любой орган внутренних дел является оператором персональных данных в силу того, что осуществляет накопление информации о гражданах. При этом в ряде случаев идет речь о специализированном накоплении информации, то есть о формировании баз данных. В ряде случаев накопление информации является результатом регистрационной деятельности, а иногда – результатом проведения оперативно-розыскных ме-

роприятий или наблюдения за оперативной обстановкой, то есть не носит систематически-целенаправленного характера.

Рассмотрим основные обязанности оператора персональных данных, которые подразделяются на следующие блоки.

Основной обязанностью здесь является предоставление субъекту персональных данных набора сведений, предусмотренных статьей 14 закона о персональных данных, а именно:

- подтверждение факта обработки персональных данных оператором, а также цель такой обработки;

- способы обработки персональных данных, применяемые оператором;

- сведения о лицах, которые имеют доступ к персональным данным или которым должен быть предоставлен такой доступ;

- перечень обрабатываемых персональных данных и источник их получения;

- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь обработка его персональных данных.

В связи с указанным, возникают два вопроса: первый связан с тем, что данное положение подразумевает формирование административного механизма его реализации, который должен содержаться в актах ведомственного уровня; второй – с тем, что для органов внутренних дел предоставление сведений о сотрудниках, имеющих доступ к персональным данным, и источниках получения персональных данных во многих случаях невозможно, а четкого права для органов внутренних дел на отказ в предоставлении вышеуказанной информации из норм закона о персональных данных не вытекает (п. 5 статьи 14 ограничивает право субъекта на доступ к своим персональным данным, но не к информации об их обработке).

Следующей обязанностью оператора является принятие необходимых организационных и технических мер для защиты персональных данных. В соответствии с п. 1 статьи 19 эти меры направлены на предотвращение неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также иных неправомерных действий в отношении этих сведений.

Степень значимости защиты персональных данных подчеркивается тем, что нормативное регулирование данных отношений не исчерпывается общей декларацией о необходимости мер защиты, а Правительству Российской Федерации законодательно предписано выработать набор требований по защите персональных данных.

Учитывая достаточно развитое нормативное регулирование в области защиты персональных данных на уровне Правительства и ведомств, уполномоченных вырабатывать в данной сфере обязательные правила,

подразумевается, что на ведомственном уровне будет обеспечена еще более детализованная нормативная база, формирующая реальный административный механизм защиты этой информации. Создание такого механизма и его устойчивое функционирование для органов внутренних дел, аккумулирующих огромное количество сведений о гражданах, является весьма актуальной задачей.

Следующим большим блоком конфиденциальной информации, с которым постоянно соприкасаются органы внутренних дел, является коммерческая тайна. Рассмотрим сущность данного правового института. Коммерческая тайна как система ограничения в доступе к информации имеет весьма древнюю историю, насчитывающую не одно тысячелетие, так как напрямую связана с отношениями конкуренции сначала на товарных, а затем и на финансовых рынках. В последний период существования Российской империи в законодательстве и юридической доктрине она именовалась как промысловая тайна и подразделялась на фабрично-заводскую и торговую тайны[1].

В советский период существования нашего государства данный институт был забыт по причине официально декларируемого отсутствия конкуренции при осуществлении социалистического производства, но существовал в виде государственной и служебной тайны в тех сферах, где государство такую конкуренцию все же поддерживало (имеется в виду прежде всего авиационная промышленность и оборонное производство).

Как легальная юридическая категория коммерческая тайна возродилась только в самом конце советского периода в Законе СССР «О предприятиях в СССР»[2], в статье 33 которого устанавливалось следующее:

«Под коммерческой тайной предприятия понимаются не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение (передача, утечка) которых может нанести ущерб его интересам».

С вступлением в действие части первой Гражданского кодекса Российской Федерации в нормативный оборот вошло определение коммерческой тайны, ставшее классическим и сохранившее свое значение до сего времени:

«Информация составляет коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности» (ч. 1 статьи 139).

---

[1] Розенберг В. Промысловая тайна – СПб., 1910. – С. 10 и далее.

[2] О предприятиях в СССР : закон СССР от 04 июня 1990 г. № 1529-I // Ведомости СНД и ВС СССР. – 1990. – № 25. – Ст. 460.

Общая идеология данного правоположения, заключающаяся в определении системного понятия через ряд признаков (а иной подход в данном случае невозможен из-за огромного многообразия отношений), сохранилась и после попыток переименования этой категории информации в «секрет производства (ноу-хау)», происшедших в связи с вступлением в силу части 4 ГК РФ в 2006 г.

Помимо регулирования на уровне Гражданского кодекса, институт коммерческой тайны имеет и специализированное регулирование в виде Федерального закона «О коммерческой тайне»[1], предмет которого в первоначальной редакции был сформулирован как регулирование отношений, связанных с отнесением информации к коммерческой тайне, передачей такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции.

Впоследствии предметная область данного законодательного акта несколько раз видоизменялась и в настоящее время заужена до регулирования отношений, связанных с установлением, изменением и прекращением режима коммерческой тайны, хотя на самом деле содержащиеся в нем нормы регулируют больший спектр правоотношений, в том числе и порядок представления сведений, составляющих коммерческую тайну, в органы публичной власти.

В отношении сведений, которые потенциально могут быть отнесены к коммерческой тайне, постоянно возникает один существенный вопрос: а насколько они должны быть защитимы государством? Авторский коллектив полагает, что настолько, насколько государство заинтересовано в развитии экономики и поддержке конкуренции как одного из существенных стимулов для роста и обеспечения качества производимых товаров, осуществляемых работ и предоставляемых услуг, то есть заинтересовано прямо и непосредственно.

Как отмечает С. В. Трофимов, «характерной чертой современной конкурентной стратегии, обеспечивающей опережающий экономический рост, стал повсеместный переход к непрерывным и динамичным инновационным процессам как собственно производства, так и способов управления производством»[2].

Развивая суждения С. В. Трофимова в плоскости настоящего исследования, авторский коллектив хотел бы отметить, что чем более инноваци-

---

[1] О коммерческой тайне : федеральный закон от 29 июля 2004 г. № 98-ФЗ // СПС «Консультант Плюс».

[2] Трофимов С. В. Правовое обеспечение инновационного развития промышленного производства. – Иркутск, 2010. – С. 4.

онной в части наукоемкости становится экономика, тем более острым становится вопрос о необходимости защиты информации от недобросовестного использования, так как оно приводит к огромным убыткам у хозяйствующих субъектов и торможению экономического развития. И органы внутренних дел должны стоять на страже данных правомерных интересов.

Однако задачи, которые решает авторский коллектив при осуществлении настоящего исследования, несколько более узкие, чем роль и место органов внутренних дел в правовой охране коммерческой тайны – в нем рассматривается проблема организации оборота и защиты данной категории сведений при правомерном попадании этой информации в подразделения органов внутренних дел.

Первый основной канал попадания – истребование данных сведений при реализации органами внутренних дел своих государственных функций. Например, истребование сведений, составляющих коммерческую тайну, у субъектов предпринимательской деятельности, осуществляющих частную охранную деятельность, торговлю оружием при осуществлении лицензирования данной деятельности.

Второй основной канал – истребование информации и изъятие ее материальных носителей при осуществлении расследования преступлений и привлечении к административной ответственности.

Третий основной канал – получение таких сведений при осуществлении оперативных мероприятий и оперативного наблюдения.

Каждый из этих каналов имеет следствием накопление сведений, составляющих коммерческую тайну, их использование и оборот в системе органов внутренних дел. Получение данных сведений органами далеко не всегда означает, что информация утратила свою коммерческую ценность и перестала быть актуальной.

Но самое основное здесь – исключить возможность утечки таких сведений из самих органов внутренних дел, а также исключить иные возможности неправомерного использования данной информации сотрудниками полиции и органами внутренних дел в целом.

Последним из блоков информации конфиденциального характера, о которых авторский коллектив должен рассказать в данном параграфе исследования, являются сведения, образующиеся при реализации задач государственной защиты. Как отмечалось выше, данную сферу общественных отношений в основном регулируют два федеральных закона:

- Федеральный закон «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»[1];

[1] О государственной защите судей, должностных лиц правоохранительных и контролирующих органов : федеральный закон от 20.04.1995 № 45-ФЗ // СПС «Консультант Плюс».

- Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»[1].

Предметом указанных федеральных законов является функция государственной защиты определенного круга физических лиц. Учитывая, что данные законодательные акты принимались в разное время, при общей схожести предмета регулирования их содержание существенно отличается друг от друга.

Важная роль в организации и реализации мер безопасности в отношении защищаемых лиц отведена органам внутренних дел. Применительно к государственной защите должностных лиц на органы внутренних дел полностью возложена защита судей, арбитражных и присяжных заседателей, прокуроров, следователей, сотрудников Следственного комитета Российской Федерации, судебных исполнителей и должностных лиц контролирующих органов, а также должностных лиц органов внутренних дел, которым необходима такая защита.

Органы внутренних дел также принимают непосредственное участие в осуществлении государственной защиты участников уголовного судопроизводства.

Таким образом, организация и реализация мер государственной защиты является одной из важных государственных задач, выполняемых органами внутренних дел, и возложена на полицию, что нашло отражение в нормах Федерального закона «О полиции»[2], п. 28 ч. 1 статьи 12 которого среди обязанностей полиции указывает осуществление государственной защиты потерпевших, свидетелей и иных участников уголовного судопроизводства, судей, прокуроров, следователей, должностных лиц правоохранительных и контролирующих органов, а также других защищаемых лиц.

Соответственно, сведения, касающиеся осуществления и содержания мер государственной защиты, являются составной частью общего массива служебной информации органов внутренних дел, их оборот должен быть упорядочен, а информационные массивы иметь адекватную защиту.

Теперь возникает необходимость в определении правовой природы сведений, касающихся государственной защиты, исходя из законодательного регулирования данных отношений. В федеральном законе о защите должностных лиц среди видов мер безопасности отдельно поименовано «обеспечение конфиденциальности сведений о защищаемых лицах», а в статье 9 данного законодательного акта раскрывается содержание этого вида мер безопасности, которое изложено следующим образом:

---

[1] О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства : федеральный закон от 20.08.2004 № 119-ФЗ // СПС «Консультант Плюс».

[2] О полиции : федеральный закон от 07 февраля 2011 года № 3-ФЗ (ред. от 12.02.2015 с изм. от 06.04.2015) // СПС «Консультант Плюс».

«По решению органа, обеспечивающего безопасность, может быть наложен временный запрет на выдачу данных о личности защищаемых лиц, их месте жительства и иных сведений о них из адресных бюро, паспортных служб, органов полиции, уполномоченных осуществлять контрольные, надзорные и разрешительные функции в отношении обеспечения безопасности дорожного движения, справочных служб автоматической телефонной связи и других информационно-справочных фондов, за исключением случаев, когда такие сведения выясняются в установленном порядке в связи с производством по уголовному делу».

Анализ вышеприведенной нормы показывает следующее. Во-первых, закон не предписывает перевод данных сведений из свободного оборота внутри соответствующего органа (организации) в состояние ограниченного доступа – запрет распространяется только на передачу сведений внешнему потребителю. Отсюда следует, что любой работник (сотрудник) организации, имеющий доступ к определенному информационному ресурсу, получает возможность знакомиться и с информацией, выдача которой во внешнюю среду ограничивается.

Во-вторых, речь идет только об информационно-справочных фондах, то есть об информационных ресурсах, специально предназначенных для накопления и структурирования в целях обеспечения возможности облегченного доступа к ним заинтересованных субъектов. Между тем речь идет о персональных данных гражданина, которые накапливаются не только в перечисленных в тексте закона информационных системах, но и во многих иных организациях (учебных заведениях, торговых организациях, организациях здравоохранения, страховых компаниях и т.д.). Соответственно, необходимо предусмотреть административный механизм изъятия необходимых сведений из любой организации, где они находятся, либо предусмотреть установление ограничений в доступе к этой информации там, где это возможно.

Закон о государственной защите участников уголовного судопроизводства трактует обеспечение конфиденциальности сведений о защищаемом лице с определенными нюансами:

«1. По решению органа, осуществляющего меры безопасности, может быть наложен запрет на выдачу сведений о защищаемом лице из государственных и иных информационно-справочных фондов, а также могут быть изменены номера его телефонов и государственные знаки используемых им или принадлежащих ему транспортных средств.

2. В исключительных случаях, связанных с производством по уголовному либо гражданскому делу, сведения о защищаемом лице могут быть представлены в органы предварительного расследования, прокуратуру или суд на основании письменного запроса прокурора или суда (судьи)

с разрешения органа, принявшего решение об осуществлении мер государственной защиты».

Общая идея обеспечения мер безопасности в виде обеспечения конфиденциальности сведений о защищаемых лицах в вышеуказанных правоположениях является одинаковой с законом об обеспечении безопасности должностных лиц, однако уровень конспирации здесь a priori выше.

Одним из самых существенных недостатков обоих законодательных актов с точки зрения настоящего исследования является то, что в них не устанавливается категорийность сведений, отражающих личность защищаемых субъектов и перечень применяемых к ним мер государственной защиты, то есть не устанавливается конкретный режим ограничения в доступе к данной информации, что резко снижает эффективность всего комплекса мероприятий. А между тем речь здесь идет об очень серьезных вещах, то есть о жизни и здоровье не только конкретного лица, но и довольно широкого круга близких ему людей, а также сохранности их имущества. Помимо указанного, речь идет о престиже государства, его способности обеспечить защиту граждан, участвующих в борьбе с преступностью и обеспечении общественной безопасности.

В любом режиме ограничения в доступе к информации центральным элементом должна выступать возможность установления точного круга лиц, которые были ознакомлены с определенной информацией. Эта возможность имеет существенное превентивное значение, так как напрямую связана с возможностью выявления и привлечения к юридической ответственности лица, допустившего утечку или разглашение информации.

В качестве заключения к данному параграфу исследования авторский коллектив хотел бы отметить следующее.

1. Анализ основополагающих законодательных актов, регулирующих отношения в сфере оборота и защиты информации, показывает, что категория «конфиденциальность» стала восприниматься в качестве синонима категории «ограничение в доступе к информации», но не как определенный класс защищаемых сведений, что вносит дисбаланс в уровни защиты информации. В связи с указанным возникает настоятельная необходимость в возрождении данного класса защищаемых сведений и определении для него четкого организационно-правового механизма защиты.

2. В связи с тем, что принятие законодательного акта, определяющего относимость сведений к служебной тайне и механизм их защиты, является делом будущего, авторский коллектив сформулировал несколько конкретных предложений по совершенствованию положения, утвержденного постановлением Правительства Российской Федерации от 03.11.1994 № 1233, заключающихся в следующем:

1) изложить п. 1.2 данного положения в следующей редакции:

«К служебной информации ограниченного распространения относятся сведения конфиденциального характера, касающиеся деятельности федеральных органов исполнительной власти и подчиненных им организаций, свободное распространение которых создает препятствия для исполнения указанными органами и организациями установленных для них задач и функций»;

2) установить в тексте положения централизованный единообразный административный механизм оборота и защиты служебной информации ограниченного распространения как на бумажных носителях, так и в электронной форме отображения, оставив для руководителей административных ведомств определение особенностей такой защиты применительно к конкретному ведомству;

3) однозначно установить, что при принятии решения об ограничении распространения определенного объема информации должен устанавливаться предельный срок введения данного ограничения, а решение о досрочном снятии ограничений должно приниматься лицом, установившим ограничения, его правопреемником либо вышестоящим руководителем.

§ 3. Сведения конфиденциального характера, накапливаемые и используемые органами внутренних дел

Рассмотрение данного комплекса вопросов целесообразно начать с анализа содержания ряда актов, касающихся организации обращения и перечней сведений, относимых в органах внутренних дел к категории сведений ограниченного распространения. Но для данных актов в целом установлена пометка «Для служебного пользования», и рассмотрение их содержания авторским коллективом в открытых источниках не представляется возможным. Считаем актуальным изучить несколько перечней сведений конфиденциального характера иных федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации и организаций, которые доступны в открытых источниках. После соотнести их с перечнем органов внутренних дел, не раскрывая содержания служебной информации ограниченного распространения последнего.

Поисковые работы, предпринятые авторским коллективом при проведении настоящего исследования, позволили обнаружить в открытых источниках значительное число перечней сведений конфиденциального характера административных ведомств федерального уровня, администраций субъектов Российской Федерации и даже отдельных организаций.

Авторский коллектив полагает, что анализ ряда положений этих актов позволит более четко выявить тенденции в отнесении сведений к категории конфиденциальных, что даст возможность более четко представить

себе направления совершенствования ведомственной нормативной базы органов внутренних дел.

Интересный образец подхода к регулированию рассматриваемых отношений представляет собой «Перечень сведений конфиденциального характера органов федерального казначейства Министерства финансов Российской Федерации», утвержденный Приказом Минфина России от 05.01.2004 № 1[1].

Обратим внимание на то, что речь идет не о служебной информации ограниченного распространения, а именно о сведениях конфиденциального характера как о более широкой категории, что и определяет содержание данного акта.

Перечень состоит из четырех разделов:

1) персональные данные;

2) сведения, связанные с исполнением функций, возложенных на органы федерального казначейства;

3) сведения по мобилизационной подготовке и гражданской обороне;

4) сведения по информатизации, организации связи и безопасности информации.

Раздел «Персональные данные» состоит из двух пунктов. Один из них является стандартным и перенесен из текста Указа Президента Российской Федерации от 06.03.1997 № 188, на который сделана ссылка в разделе «Примечание», а второй сформулирован следующим образом:

«Сведения, содержащиеся в личных делах сотрудников или в анкетах, или в паспорте, или в иных документах, позволяющие идентифицировать личность гражданина».

Таким образом, сведения о фактах, событиях и обстоятельствах частной жизни граждан, которые могут быть представлены в любой форме отображения, довольно юридически корректно разграничены с документами, содержащими аналогичные сведения.

Еще более оригинальный подход предложен разработчиками данного акта при формулировании категорий конфиденциальной информации, объединенных во втором разделе перечня. Например, п. 2.1 сформулирован следующим образом:

«Сведения организаций и предприятий, ставшие известными сотрудникам органов федерального казначейства при выполнении служебных обязанностей, которые этими предприятиями и организациями отнесены к конфиденциальным».

Из контекста данного положения следует, что если организация предупредила сотрудника казначейства о конфиденциальности информации,

---

[1] Перечень сведений конфиденциального характера органов федерального казначейства Министерства финансов Российской Федерации : приказ Минфина России от 05.01.2004 г. № 1 // СПС «Консультант Плюс».

то он обязан соблюдать условия конфиденциальности. Несомненно, данное положение является актуальным для органов внутренних дел и должно быть включено в соответствующий перечень сведений конфиденциального характера.

Представляет интерес тот факт, что в качестве основания для данной нормы представлена статья 727 ГК РФ, которая сформулирована следующим образом:

«Если сторона благодаря исполнению своего обязательства по договору подряда получила от другой стороны информацию о новых решениях и технических знаниях, в том числе не защищаемых законом, а также сведения, в отношении которых их обладателем установлен режим коммерческой тайны, сторона, получившая такую информацию, не вправе сообщать ее третьим лицам без согласия другой стороны».

По мнению авторского коллектива, никаких договорных отношений между сотрудником федерального органа исполнительной власти и организацией, связанных с исполнением государственных функций, возникнуть не может, поэтому применение данного законодательного положения является вынужденным, связанным с дефицитом законодательного регулирования отношений в сфере оборота и защиты конфиденциальной информации.

В соответствии с принципом, описанным авторским коллективом выше, согласно которому сведения в любой форме отображения обособляются от документированных сведений, сформулирован и п. 2.2 рассматриваемого перечня:

«Сведения, содержащиеся в документах юридического дела бюджетополучателей и распорядителей бюджетных средств, имеющих лицевые счета в органах федерального казначейства, в «Книге регистрации лицевых счетов», в карточке с образцами подписей и оттисками печатей распорядителей бюджетных средств».

Данная норма представляет определенный интерес и по той причине, что она в существенной мере схожа с банковской тайной, в режиме которой защищаются сведения о наличии и движении денежных средств по счетам банковской системы. Но дело здесь несколько сложнее, так как получателями бюджетных средств являются все без исключения органы государственной власти и организации, в том числе относящиеся к категории особо режимных, то есть таких, сам факт существования которых легендируется. Из этого следуют дополнительные основания для признания вышеуказанной информации конфиденциальной.

Далее следует очень важная норма, которая должна быть предметом перечня сведений конфиденциального характера любого федерального органа исполнительной власти, а равно и любого другого органа публичной власти:

«Сведения, поступающие в органы федерального казначейства от сторонних организаций, отнесенные этими организациями в установленном порядке к конфиденциальным (налоговая тайна, таможенная тайна, конфиденциальные сведения Пенсионного фонда и т. п.)».

Факт признания такой информации конфиденциальной является одним из важнейших условий существования всей системы легального оборота таких сведений в органах публичной власти и, естественно, должен иметь следствием подпадание поступающих сведений под определенный защитительный режим.

Содержание следующего за вышеуказанным пункта несколько дезавуирует общее благоприятное впечатление от анализируемого перечня. Пункт 2.5 относит к числу конфиденциальной информации «сведения, содержащиеся в документах с пометкой “Для служебного пользования”».

У данной нормы есть как бы два полюса – положительный и отрицательный. Положительный полюс заключается в том, что сведения «Для служебного пользования» легально признаются конфиденциальной информацией, а не неким обособленным классом сведений, как это позиционируется, в частности, в рассмотренном выше примерном перечне МВД России. Отрицательный полюс состоит в том, что сведения «Для служебного пользования» приобщаются к некоему ряду конфиденциальной информации без акцента на то, что для них существует обособленный режим защиты, в связи с чем возникает резонный вопрос: а каковы контуры и содержание режима защиты сведений конфиденциального характера в органах федерального казначейства?

Как представляется авторскому коллективу, таких контуров не имеется, а имеется лишь факт признания сведений конфиденциальными.

Еще более запутанную ситуацию в части определения того, а что же, собственно, может относиться к сведениям «Для служебного пользования», создает следующий пункт рассматриваемого перечня:

«Сведения об организации, состоянии или проводимых мероприятиях по мобилизационной подготовке или гражданской обороне в органах федерального казначейства, если такие сведения не отнесены в установленном порядке к сведениям, составляющим государственную тайну».

Сведения по мобилизационной работе являются во всех случаях сугубо служебными и обычно в органах государственной власти, в том числе и в системе МВД России, присутствует четкая корреляция между перечнем сведений, составляющих государственную тайну (подлежащих засекречиванию), и перечнем сведений ограниченного распространения в части того, на каком уровне административного управления и какие сведения ограничиваются в доступе и распространении пометкой «Для служебного пользования», а на каком признаются сведениями, составляющими государственную тайну.

Примерно в том же ключе следует трактовать и блок защищаемых сведений, касающихся организации связи и безопасности информации. Например, сведения об организации разграничения доступа к информационным ресурсам органов федерального казначейства, паролях, закрытых ключах ЭЦП, ключах шифрования информации, которые не относятся к государственной тайне, признаются конфиденциальными. Это правильно, однако в каком режиме осуществляется оборот этих сведений, каков административный механизм обеспечения персональной ответственности за их сохранность и исключение противоправного распространения?

Доступные для открытого ознакомления ответы на данный вопрос нормативные акты Федерального казначейства и Минфина России в целом не дают. Но ведь речь идет об очень важной для современных условий информации, связанной с обеспечением безопасного движения денежных средств в безналичной форме, предотвращения противоправных действий по отношению к ним.

Следует отметить, что для государственной финансовой системы данная ситуация является не уникальной – эту частично ошибочную логику воспринял и «Перечень сведений ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера) Министерства финансов Российской Федерации», утвержденный Приказом Минфина России от 17.06.2014 № 162[1]. Однако в данном акте имеются и положения, заслуживающие внимания с точки зрения ареала информации, относимой к категории конфиденциальной, в федеральных органах исполнительной власти. Например, данный акт совершенно справедливо относит к данной категории «сведения, содержащие персональные данные, обрабатываемые в Министерстве финансов Российской Федерации, в рамках реализации функций и полномочий федерального органа исполнительной власти».

По мнению авторского коллектива, такой пункт крайне необходим в перечне сведений конфиденциального характера органов внутренних дел.

Следующей нормой, которую до сего времени не восприняли ведомственные нормативные правовые акты, регулирующие отнесение сведений к категории конфиденциальной, являются «сведения о первичных статистических данных, содержащиеся в формах федерального статистического наблюдения, сбор и обработка которых осуществляется субъектами официального статистического учета в целях формирования официальной статистической информации в установленной сфере деятельности». Данное положение включено в перечень Минфина России и имеет основанием нормы

[1] Перечень сведений ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера) Министерства финансов Российской Федерации : приказ Минфина России от 17.06.2014 № 162 // СПС «Консультант Плюс».

статьи 9 Федерального закона «Об официальном статистическом учете и системе государственной статистики в Российской Федерации»[1], которая признает данный вид информации сведениями ограниченного доступа. Причем речь в указанном законе идет не только о первичных статистических данных как «документированной информации по формам федерального статистического наблюдения, получаемой от респондентов либо документируемой непосредственно в ходе федерального статистического наблюдения», но и об административных данных, под которыми понимается «документированная информация, получаемая федеральными органами исполнительной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления и государственными организациями в связи с осуществлением ими разрешительных, регистрационных, контрольно-надзорных и других административных функций».

Данный важный класс информации, законодательно определенный как конфиденциальный, полностью упущен из поля зрения в органах внутренних дел, где таких сведений огромное количество.

В рассматриваемый перечень Минфина России включено, но, к сожалению, полностью упущено примерным перечнем МВД России, положение о том, что к категории конфиденциальной информации относятся «сведения, содержащиеся в заявках, поданных в форме электронных документов на участие в открытом конкурсе».

Данное положение вытекает из норм статьи 51 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»[2]. Пункт 11 данной статьи содержит следующее положение:

«Заказчик, специализированная организация обеспечивают сохранность конвертов с заявками на участие в открытом конкурсе, защищенность, неприкосновенность и конфиденциальность поданных в форме электронных документов заявок на участие в открытом конкурсе и обеспечивают рассмотрение содержания заявок на участие в открытом конкурсе только после вскрытия конвертов с заявками на участие в открытом конкурсе или открытия доступа к поданным в форме электронных документов заявкам на участие в открытом конкурсе в соответствии с настоящим федеральным законом. Лица, осуществляющие хранение конвертов с заявками на участие в открытом конкурсе, в том числе поданных в форме электронных документов заявок на участие в открытом конкурсе, не вправе

[1] Об официальном статистическом учете и системе государственной статистики в Российской Федерации : федеральный закон от 29.11.2007 № 282-ФЗ // СПС «Консультант Плюс».

[2] О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд : федеральный закон от 05.04.2013 № 44-ФЗ // СПС «Консультант Плюс».

допускать повреждение этих конвертов, осуществлять открытие доступа к таким заявкам до момента вскрытия конвертов с заявками на участие в открытом конкурсе или открытия доступа к поданным в форме электронных документов заявкам на участие в открытом конкурсе в соответствии с настоящим федеральным законом».

Проведенный небольшой сравнительный анализ показывает как несовершенство всей системы отнесения сведений к категории конфиденциальных в системе органов исполнительной власти, которой явно не хватает единой доктринальной платформы и должного законодательного регулирования, так и отсутствие какого-либо системного подхода к регулированию данных отношений в МВД России, где ведомственное регулирование существенным образом отстает от развивающегося законодательного регулирования.

Развитие отношений в области формализации отнесения сведений к категории конфиденциальных осуществляется не только на уровне федеральных органов исполнительной власти, но и на уровне органов государственной власти субъектов Российской Федерации, многие из которых приняли соответствующие акты в разные периоды времени. Так, в частности, в администрации Омской области перечень сведений конфиденциального характера действует с 1998 г. (утвержден распоряжением главы администрации (губернатора) Омской области от 08.01.1998 № 9-р[1]).

Прежде чем приступить к анализу отдельных положений данного перечня, следует обратить внимание на весьма здравую логику самого распоряжения, которое распространяет пометку «Для служебного пользования» на все сведения конфиденциального характера вне зависимости от их правовой природы (будь то служебная информация ограниченного распространения, сведения, отнесенные к коммерческой тайне, или персональные данные).

Довольно кратко и логично решается вопрос и относительно правомочия наложения ограничений на распространение сведений, а также снятия таких ограничений:

- простановка пометки «Для служебного пользования» осуществляется руководителями комитетов, управлений и отделов администрации области;

- снятие пометки «Для служебного пользования» осуществляется лицом, подписавшим документ, либо вышестоящими руководителями.

Интересен также подход к порядку и условиям принятия решений о распространении сведений конфиденциального характера:

- для сведений, составляющих служебную тайну, на данное действие требуется разрешение губернатора области, его заместителей либо управляющего делами администрации области;

---

[1] Перечень сведений конфиденциального характера : распоряжение главы администрации Омской области от 08.01.1998 № 9-р // СПС «Консультант Плюс».

- для персональных данных – разрешение соответствующего физического лица;

- для сведений, составляющих коммерческую тайну, – разрешение хозяйствующего субъекта, являющегося обладателем этих сведений.

Анализ содержательной части перечня сведений конфиденциального характера, утвержденного вышеуказанным распоряжением, показывает существенную его недоработанность с точки зрения юридической доктрины и лишний раз подчеркивает необходимость регулирования данных отношений на уровне федерального закона, что позволило бы снять различного рода заблуждения.

Однако начнем с положительных моментов, к которым относится включение в состав перечня категорий сведений, касающихся персональных данных и коммерческой тайны субъектов предпринимательской деятельности. Первое, на что следует обратить внимание – это категория «сведения о фактах, событиях и обстоятельствах частной жизни граждан, обращающихся в подразделения администрации области». На такой информации простановка пометки «Для служебного пользования» является обязательной.

В данном случае является принципиально важным уяснить, что именно относится к частной жизни граждан. Разъяснений по этому поводу не дается, из чего следует, что работники аппарата администрации области будут опытным путем отделять частное от публичного в обращениях граждан. Однако это разрешимая задача, так как подавляющее большинство взрослых людей, имеющих нормальное интеллектуальное развитие, в состоянии достаточно четко очертить границы частной сферы человеческого бытия.

По мнению авторского коллектива, данное правоположение должно стать предметом соответствующих перечней конфиденциальной информации в органах внутренних дел на всех уровнях, так как они аккумулируют огромное число сведений частного характера, передаваемых полиции в виде различных обращений, в том числе заявлений.

Вне всякого сомнения, к категории персональных данных относятся и записи актов гражданского состояния, на которых предусмотрено в обязательном порядке проставление пометки «Для служебного пользования», как это указано в рассматриваемом перечне администрации Омской области.

Напротив, сведения о недвижимости, находящейся в частной собственности граждан, в том числе данные земельного кадастра, не могут быть предметом ограничений, как это предусмотрено рассматриваемым перечнем – в противном случае будут блокированы многие вопросы гражданского оборота недвижимого имущества.

Хотя ограничения на распространение сведений из медицинских карт служащих подразделений администрации области устанавливаются не в обязательном порядке, а по решению лица, исполняющего документ,

сам факт появления данного положения в перечне следует признать позитивным фактом, равно как и наложение ограничений на распространение сведений, содержащихся в декларациях и других документах о соблюдении гражданами ограничений, связанных с замещением государственных должностей.

Применительно к коммерческой тайне в перечень включены два положения:

1) «сведения, содержащие коммерческую тайну хозяйствующих субъектов, переданные подразделениям администрации области»;

2) «сведения, содержащие данные статистической отчетности хозяйствующих субъектов области».

По мнению авторского коллектива, данных правоположений достаточно для охвата всей совокупности сведений, касающихся коммерческой тайны. Для органов внутренних дел, легально получающих огромное число сведений, составляющих коммерческую тайну субъектов предпринимательской деятельности, необходимо формирование отдельного раздела в Перечне сведений конфиденциального характера, в котором была бы описана совокупность этой информации по видам, способам получения и объему.

Авторский коллектив также позитивно относится к установлению ограничений на распространение, как это установлено рассматриваемым перечнем, различных проектов актов и документов до их официального опубликования, так как это может привести к негативным последствиям в виде паники на региональных ранках и т.п.

Однако нельзя согласиться с авторами перечня относительно включения в него следующих позиций:

1. «Сведения, раскрывающие условия получения областью зарубежных кредитов».

По мнению авторского коллектива, является весьма странным, что такая информация вообще может скрываться, так как речь идет не о частной компании, а о публичном образовании в виде субъекта федеративного государства.

2. «Информация об условиях аренды или продажи государственной собственности области».

По мнению авторского коллектива, попытка скрыть такую информацию ведет прежде всего к увеличению коррупционной составляющей в деятельности государственной власти, когда под «покровом тайны» идет распродажа государственного имущества «нужным» людям и организациям.

3. «Сведения, раскрывающие содержание мероприятий по закупкам и продаже (поставкам) зерна, сырья, материалов, топлива, оборудования, средств защиты сельскохозяйственных животных и растений».

Из данного положения следует, что любая информация, связанная с движением материальных ценностей внутри области и за ее пределы автоматически становится конфиденциальной. Буквальное выполнение данного правоположения может блокировать огромные информационные потоки без какого-либо разумного (с точки зрения ограничения в доступе к информации) основания.

Следует также обратить внимание на тот факт, что рассматриваемый перечень практически полностью игнорирует правоохранительную деятельность, хотя она является важным составным элементом в работе администрации любого субъекта Российской Федерации.

Анализ перечней сведений других субъектов Российской Федерации показывает существенную разницу как в подходах к объемам защищаемой информации, так и в системе построения перечней. Так, в частности, Перечень сведений конфиденциального характера в администрации Волгоградской области, утвержденный постановлением главы администрации данного региона от 24.01.2006 № 54[1], содержит всего десять позиций, из которых половина касается защиты персональных данных. По мнению авторского коллектива, перечень такого объема малопригоден для практического использования.

По мнению авторского коллектива настоящего исследования, сведения конфиденциального характера о правоохранительной деятельности образуются в деятельности администраций субъектов Российской Федерации постоянно и в силу этого должны быть предметом соответствующих перечней. Инициатором содержательной части такого блока сведений должно централизованно выступить МВД России, выйдя с ходатайством в Правительство Российской Федерации об обязывании администраций (правительств) субъектов Российской Федерации включить в перечни соответствующие позиции.

Следует отметить, что практика формирования перечней сведений конфиденциального характера имеет место не только на уровне административных ведомств федерального уровня или органов государственной власти субъектов Российской Федерации, но и на уровне муниципальных образований. Интересный образец такого акта представляет собой «Перечень сведений конфиденциального характера администрации Мариинского муниципального района, отраслевых (функциональных) органов администрации Мариинского муниципального района и подведомственных им

[1] Перечень сведений конфиденциального характера : постановление главы администрации Волгоградской области от 24.01.2006 № 54 // СПС «Консультант Плюс».

учреждений» (Кемеровская область), утвержденный постановлением главы администрации данного района от 07.05.2013 № 438-П[1].

Например, в данном перечне в качестве конфиденциальных признаются «сведения, прямо или косвенно указывающие на личность несовершеннолетнего, совершившего преступление либо подозреваемого в его совершении, а равно совершившего административное правонарушение или антиобщественное действие, без согласия самого несовершеннолетнего или его законного представителя».

Неясно, что явилось основанием для введения данного положения, но оно не лишено здравого смысла, так как направлено на защиту информации о личности гражданина.

Далее, конфиденциальной признается «переписка администрации Мариинского муниципального района, отраслевых (функциональных) органов администрации и подведомственных им учреждений с территориальными органами ФСБ России, МВД России, Минобороны России, МЧС России, ФСТЭК России, ФСО России, прокуратурой Кемеровской области, прокуратурой города Мариинска». Как представляется авторскому коллективу, признание всей без исключения переписки с указанными административными ведомствами конфиденциальной является неправомерным решением, так как она может носить совершенно открытый характер, и попытка ограничить к таким документам доступ может только навредить правильному разрешению обозначенных в них вопросов.

К числу позитивных моментов в содержательной части перечня администрации Мариинского района можно отнести положение о признании конфиденциальными сведений, содержащихся в материалах служебных расследований «до издания соответствующих распорядительных документов».

По мнению авторского коллектива, акценты в данном положении расставлены совершенно правильно: пока публичное решение не принято, информация не оглашается; после принятия решения доступ к материалам становится открытым.

Поиск, осуществленный в процессе исследования, показал, что муниципальные образования не являются самым нижним уровнем управления, на котором осуществляется разработка перечней сведений конфиденциального характера. В открытом доступе в Интернете авторским коллективом был обнаружен Перечень сведений конфиденциального характера муниципального дошкольного образовательного учреждения «Мало-Шелемишевский детский сад» Скопинского муниципального района Ря-

[1] Перечень сведений конфиденциального характера : постановление главы администрации Мариинского муниципального района от 07.05.2013 № 438–П // СПС «Консультант Плюс».

занской области, утвержденный приказом директора данного учреждения от 29.07.2013 № 15[1], представляющий по ряду позиций научный интерес.

К числу позитивных моментов можно отнести признание конфиденциальными персональных данных воспитанников детского сада (заметим – с постоянным сроком хранения в данном качестве); сведений об усыновителях, приемных родителях и опекунах; сведений об охране учреждения, системе сигнализации, наличии средств контроля и управления доступом в учреждение. К числу явно негативных с точки зрения правомерности-неправомерности ограничения в доступе можно отнести следующие позиции:

- сведения, содержащиеся в финансово-договорных схемах учреждения;

- сведения об используемой в коллективе системе стимулов, укрепляющих дисциплину, повышающих производительность труда;

- информацию о личных отношениях специалистов как между собой, так и с руководством, сведения о возможных противоречиях, конфликтах внутри коллектива.

В отношении первой из приведенных позиций следует отметить, что муниципальные учреждения содержатся на деньги налогоплательщиков, поэтому ограничение в доступе к сведениям, содержащимся в финансово-договорных схемах, неправомерно и может привести к злоупотреблениям при расходовании бюджетных средств.

Стимулирование труда в организации, содержащейся на публичные деньги и не являющейся коммерческой, также не может осуществляться под покровом конфиденциальности.

Из третьей позиции правомерно лишь отнесение к категории конфиденциальной информации сведений о личных отношениях специалистов между собой. Отношения работника и представителя работодателя носят публичный характер и не могут официально ограничиваться в доступе. Эта информация, как и информация о конфликтах, может скрываться только по договоренности между сторонами данного конфликта.

Проведенный авторским коллективом небольшой анализ со всей очевидностью показывает, что упорядочение отношений в части обособления конфиденциальной информации от остального информационного массива является велением времени и происходит не только в органах государственной власти или органах местного самоуправления, но и в организациях такого уровня, о наличии в которых сведений ограниченного доступа и помыслить ранее было невозможно.

---

[1] Перечень сведений конфиденциального характера муниципального дошкольного образовательного учреждения «Мало-Шелемишевский детский сад» Скопинского муниципального района Рязанской области : приказ директора от 29.07.2013 № 15 // URL: www.shelemishevsad.ucod.ru.

Органы внутренних дел в этой деятельности уступают, прежде всего, из-за устаревшего перечня, детальный анализ которого в открытой научной литературе невозможен. Создавшееся положение необходимо исправлять.

Одним из реализуемых ныне путей решения данного вопроса является создание двухуровневой системы перечней сведений конфиденциального характера, как это сделано в Республике Беларусь в соответствии с постановлением Совета Министров Республики Беларусь от 12.08.2014 № 783[1].

Первый уровень здесь общегосударственный перечень. Второй уровень – ведомственные перечни, которые не могут противоречить общегосударственному.

Общегосударственный перечень утвержден наряду с положением о порядке ведения делопроизводства по документам, содержащим такую информацию, вышеуказанным постановлением и поделен на разделы, один из которых поименован как «Правоохранительная деятельность». Анализ ряда положений данного раздела поможет нам представить круг сведений, который в Белоруссии относят к категории конфиденциальных в данной области общественных отношений.

Собственно к деятельности милиции в данном государстве относятся только четыре пункта:

- сведения, связанные с профессиональной деятельностью, разглашение которых может создать угрозу личной безопасности сотрудников правоохранительных органов и членов их семей, их имуществу;
- сведения о силах, средствах, формах и методах ведения предварительного расследования;
- сведения, содержащие результаты взаимодействия оперативных подразделений правоохранительных органов при выявлении (раскрытии) преступлений;
- сведения о дислокации постов и маршрутов патрулирования нарядами ДПС ГИБДД МВД.

Анализ приведенных выше категорий показывает тщетность попыток установления перечня сведений ограниченного распространения на общегосударственном уровне – при более детальном регулировании такой перечень получился бы слишком громоздким.

Таким образом, задача общегосударственного уровня правового регулирования заключается прежде всего в выработке научно обоснованных критериев отнесения сведений к данной категории, исключающих посягательства на права и свободы человека и гражданина, а затем в установле-

[1] О служебной информации ограниченного распространения : постановление совета министров Республики Беларусь от 12.08.2014 № 783 // Национальный правовой интернет-портал Республики Беларусь. 16.08.2014, 5/39265.

нии общих, фундаментальных и единых рамок режима защиты такой информации с правом детализации отдельных методов и способов на уровне административных ведомств.

Первое из приведенных положений представляется авторскому коллективу важным для упорядочения оборота служебной информации в органах внутренних дел. Однако не все такие сведения могут быть предметом служебной тайны. Существенная часть из них должна являться предметом государственной тайны и на органическую связь между данными институтами применительно к указанным категориям сведений следовало бы сделать соответствующий акцент.

Вторая из приведенных категорий имеет в Российской Федерации собственное название – институт тайны предварительного расследования. В принципе, распространение на этот блок информации единого режима сведений ограниченного распространения, по мнению авторского коллектива, носит позитивный характер, так как уголовно-процессуальным законодательством система реального ограничения доступа при обороте такой информации практически не устанавливается, отдавая все решения на ограничение в доступе на усмотрение лиц, осуществляющих предварительное расследование. Теперь Беларусь вышла из этой неопределенности, а Россия в ней осталась.

Следующий из процитированных выше пунктов касается исключительно оперативной работы. В целом следует позитивно оценить стремление упорядочить оборот данной информации, но грань между служебной и государственной тайнами в данной сфере является очень тонкой, поэтому было бы правильным добавить «если эти сведения не составляют государственной тайны».

Таким образом, пометка «Для служебного пользования» будет предельно нижним уровнем для ограничения в доступе к такого рода информации.

Наконец, сведения о дислокации постов и карты маршрутов. Для инспекции безопасности дорожного движения это, конечно, важно, но не менее важным является обеспечение защиты такой информации и для патрульно-постовой службы. Во всяком случае, если данное положение распространять на российскую правовую почву, то следует поступать именно таким образом.

Проведенный анализ показывает в целом верный подход разработчиков белорусского перечня к регулированию данных отношений, однако он носит заведомо фрагментарный характер, что приводит авторский коллектив настоящего исследования к убеждению в том, что необходимо разрабатывать развернутые ведомственные перечни, где по каждому направлению деятельности административного ведомства, определенному соответствующим положением о нем, устанавливать категории служебной инфор-

мации, доступ к которым должен быть ограничен в режиме служебной тайны.

Завершая рассмотрение белорусского перечня сведений ограниченного распространения в части правоохранительной деятельности, авторский коллектив решил коснуться одной казусной позиции, а именно категории, согласно которой ограничивается распространение информации «об объемах отпуска хлебопродуктов спецпотребителям (исправительным учреждениям) в ассортименте». Для авторского коллектива остается загадкой, почему вообще данная информация ограничивается в доступе и распространении и почему речь идет только о хлебопродуктах, но не о продуктах питания в целом. Это наглядный пример ничем не обоснованного ограничения в доступе к информации.

Интерес представляет также дополнение перечня сведений в системе МВД России, которые не могут быть отнесены к служебным сведениям, предпринятое разработчиками положения, в сравнении с аналогичным перечнем из текста положения, утвержденного Постановлением Правительства Российской Федерации от 03.11.1994 № 1233: «запрещено относить к служебным сведениям описание структуры МВД России, его функций, направлений и форм деятельности, а также адрес МВД России». Говоря иначе, указанная информация должна быть полностью общедоступной.

При анализе данного положения сразу возникает несколько вопросов. Первый заключается в следующем: если раскрывается структура самого министерства, то по логике должна раскрываться структура любого органа внутренних дел, но об этом ничего не сказано. Второй вопрос заключается в следующем: до какого предела раскрывается структура министерства – до структурного подразделения, до подразделения, входящего в состав структурного подразделения, до отдельной должности сотрудника с описанием его должностных обязанностей или как-то иначе?

Тем не менее можно констатировать, что в целом (применительно к МВД России) данный пункт выполняется и любой гражданин может получить довольно целостное представление о структуре аппарата Министерства внутренних дел.

Например, сайт Главного управления МВД России по Воронежской области www.36.мвд.рф содержит довольно подробную информацию о структуре данного областного органа, за исключением ряда подразделений, которые не влияют на абрис его общей структуры. Однако описание функциональных задач подразделений дается схематично, что в ряде случаев порождает искаженное представление об их предназначении.

Фрагментарный и непоследовательный подход к регулированию отношений в области отнесения сведений к категории конфиденциальных в органах внутренних дел можно проиллюстрировать еще одним примером. В соответствии с п. 29 статьи 13 Федерального закона «О полиции» поли-

ция вправе «получать в целях предупреждения, выявления и раскрытия преступлений в соответствии с законодательством Российской Федерации сведения, составляющие налоговую тайну».

Налоговая тайна является одной из разновидностей профессиональной тайны, а в части правовой природы защищаемой в данном режиме информации применительно к физическим лицам – персональными данными, применительно к юридическим лицам – коммерческой тайной.

В основе системы правового регулирования в сфере налоговой тайны лежат нормы статьи 102 НК РФ, согласно которым налоговую тайну составляют любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственного внебюджетного фонда и таможенным органом сведения о налогоплательщике» (в основном данные налогового учета, в том числе содержание первичных документов).

Основная потенциальная опасность от противоправного распространения такой информации заключается для физического лица в том, что третьи лица могут получать целостное представление о его реальном имущественном, в том числе финансовом положении; для юридического лица – в том, что через данные налогового учета могут стать известными сведения, составляющие коммерческую тайну данного субъекта.

Проведенный авторским коллективом анализ показал, что весь административный механизм защиты данной информации в органах внутренних дел сводится к формированию Перечня должностных лиц системы МВД России, пользующихся правом доступа к сведениям, составляющим коммерческую тайну. В настоящее время действует перечень, утвержденный Приказом МВД России от 11.01.2012 № 17[1].

Все должностные лица в этом перечне подразделяются на тех, кто имеет доступ к данной информации в полном объеме и тех, кто имеет доступ к ней «в объеме, необходимом для выполнения должностных обязанностей, определенных положениями о соответствующих подразделениях и должностными инструкциями».

Приказ не дает градации того, что означает доступ в полном объеме или необходимом объеме. По мнению авторского коллектива, в полном объеме означает то, что должностное лицо имеет возможность доступа к налоговой информации о любом физическом или юридическом лице без ограничения, в необходимом объеме – в связи с проведением определенных оперативных или иных служебных мероприятий, что в ряде случаев трудно отличить от полного объема.

Анализ содержания перечня показывает, что в полном объеме к этой информации в основном имеют доступ руководители МВД России и руко-

[1] Об утверждении Перечня должностных лиц системы МВД России, пользующихся правом доступа к сведениям, составляющим налоговую тайну : приказ МВД России от 11.01.2012 № 17 (ред. от 03.04.2014) // СПС «Консультант Плюс».

водители оперативных главков и департаментов. Непонятно, однако, какое отношение к данным сведениям (да еще в полном объеме) имеет начальник отдела уголовного законодательства и правового регулирования предупреждения преступлений уголовно-правового управления Договорно-правового департамента МВД России, который явно не занимается оперативной работой и не проводит следственных действий.

Авторскому коллективу настоящего исследования, к сожалению, не удалось обнаружить каких-либо актов, определяющих порядок доступа к сведениям, составляющим налоговую тайну, порядок и сроки хранения полученной информации в системе МВД России, порядок ее передачи между подразделениями органов внутренних дел и т.д., то есть всего того, что характеризует содержание понятия «оборот информации». И это явный пробел в правовом регулировании данных отношений на ведомственном уровне.

В качестве заключения к данному параграфу исследования хотелось бы отметить следующее:

1. Результат анализа нескольких перечней сведений конфиденциального характера иных федеральных органов исполнительной власти, органов государственной власти субъектов Российской Федерации и организаций, предпринятого авторским коллективом для сравнения с Примерным перечнем МВД России, подтверждает отсутствие единого системного подхода в части формирования их содержания, что является дополнительной иллюстрацией необходимости принятия федерального закона, имеющего целью упорядочить оборот и обеспечить защиту этой информации.

2. В настоящее время практически все органы государственной власти субъектов Российской Федерации разработали перечни сведений конфиденциального характера. Учитывая, что борьба с преступностью и обеспечение общественной безопасности являются задачей не только органов внутренних дел, но и вышеуказанных органов, по мнению авторского коллектива, необходимо в каждый такой перечень включить раздел «Правоохранительная деятельность». В целях исключения разночтений в формировании его содержательной части целесообразно было бы определить разработчиком основных норм данного раздела МВД России, а внести такие изменения отдельным постановлением Правительства Российской Федерации.

3. Уровень ведомственного нормативного регулирования отношений в сфере обеспечения сохранности информации о налогоплательщиках (налоговой тайны), обеспечиваемый в системе МВД России, наглядно иллюстрирует отсутствие концепции защиты конфиденциальной информации в органах внутренних дел, так как при определении субъектов, имеющих доступ к этим сведениям, не определяется порядок обеспечения сохранности такой информации в ее документальном отображении, порядок ее оборота в органах внутренних дел и ответственность должностных лиц за ее противоправное распространение.

§ 4. Административно-правовое регулирование внутрисистемной и внесистемной передачи сведений конфиденциального характера в органах внутренних дел

Начать анализ системы оборота конфиденциальной информации в органах внутренних дел следует с утверждения о том, что система защиты данной информации является центральным элементом общей системы оборота конфиденциальных сведений. Вторым центральным элементом является обеспечение возможности реального доступа к банкам такой информации уполномоченных лиц.

В качестве примера для анализа возьмем некоторые аспекты ведомственной целевой программы «Сельский участковый», утвержденной Приказом МВД России от 19.11.2013 № 919[1].

С сельского участкового начинается вся система органов внутренних дел. Он является также субъектом служебного информационного обмена, так как предоставляет определенную информацию в банки данных органов внутренних дел и по логике должен иметь доступ к содержанию определенного числа таких банков. Посмотрим, какими средствами согласно данной программе будет обладать сельский участковый, чтобы участвовать в информационном обмене. Как следует из приложения № 1 к данному приказу, каждому участковому положен один стационарный компьютер, один монохромный принтер и один интегрированный офисный аппарат на каждый участковый пункт полиции. Каждому участковому также положена одна носимая радиостанция. Возимой радиостанцией оснащается каждый оперативно-служебный автомобиль, стационарной – каждый участковый пункт полиции.

Ни о каких средствах, позволяющих подключаться к информационно-телекоммуникационной сети Интернет, и ни о каких средствах защиты информации в данной обширной программе, предусматривающей даже надувные лодки и наручники, речи не идет, в силу чего можно сделать вывод о том, что сельский участковый уполномоченный полиции в обозримом будущем не будет являться активным участником служебного информационного обмена в органах внутренних дел.

А между тем проблема формирования единого информационного пространства органов внутренних дел далеко не нова. В Приказе МВД России от 20.05.2008 г. № 435 «Об утверждении новой редакции программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел» совершенно справедливо отмечалось следующее:

---

[1] Об утверждении ведомственной целевой программы «Сельский участковый» : приказ МВД России от 19.11.2013 № 919 // СПС «Консультант Плюс».

«Для решения стоящих перед органами внутренних дел задач МВД России разработан и реализуется комплекс мер по адекватному противодействию криминальным и нелегальным миграционным процессам, терроризму, экстремизму, эффективной защите прав и свобод граждан, обеспечению охраны общественного порядка, неукоснительному исполнению в части, касающейся международных обязательств России.

Однако, несмотря на постоянный рост и усложнение задач, стоящих перед МВД России, при неизменном штатном составе органов внутренних дел, а также ряд объективных проблем, в первую очередь связанных с недостаточным материально-техническим и кадровым обеспечением, решение указанных задач в значительной мере затруднено. Поэтому МВД России принимает меры по ослаблению негативного влияния имеющихся проблем на реализацию задач, стоящих перед органами внутренних дел, путем повышения уровня организации управления и эффективности использования имеющихся сил и средств.

Одним из основных направлений реализации указанных мер является совершенствование информационного обеспечения органов внутренних дел на основе оснащения их современными аппаратно-программными комплексами и системами, а также внедрение в практическую деятельность новых и перспективных информационных технологий.

МВД России постоянно проводит мероприятия в этом направлении в рамках выделяемых из федерального бюджета финансовых средств, а также привлекая для решения указанной задачи средства региональных и местных бюджетов. Добавим к этому, что эффективный информационный обмен существенно ускоряет процессы раскрытия и расследования преступлений, существенно снижает общие сроки содержания граждан под стражей, позволяя быстрее устанавливать необходимые факты, и имеет много иных позитивных следствий.

Среди многочисленных позитивных результатов формирования ЕИТС авторский коллектив хотел бы особенно выделить следующие:

- сокращение времени и моральных издержек розыска и изобличения лиц, совершивших преступления или причастных к их совершению, предоставление оперативным сотрудникам органов внутренних дел новых технических возможностей по повышению эффективности оперативно-служебной деятельности;

- сокращение времени обработки и выдачи официальной юридически легитимной информации, являющейся доказательной базой при раскрытии преступлений, в том числе предоставление новых технических возможностей получения процессуальной доказательной базы при расследовании нераскрытых преступлений прошлых лет.

Представляет научный интерес набор мер, которые, по мнению разработчиков данной программы, обеспечивают гарантированный уровень

информационной безопасности при информационно-телекоммуникационном обеспечении деятельности органов внутренних дел.

Обеспечение информационной безопасности, как следует из текста концепции, достигается выполнением следующих функций по защите информации:

- идентификация и аутентификация пользователей;
- разграничение доступа к информационным и техническим ресурсам;
- межсетевое экранирование;
- криптографическая защита информационного обмена;
- антивирусная защита;
- предотвращение утечки информации за счет побочных излучений и наводок;
- обеспечение возможности электронной цифровой подписи для обеспечения электронного юридически значимого оборота.

Из всех перечисленных функций только три имеют правовую составляющую, а на обеспечение защиты информации от противоправного распространения с включением в систему такого элемента, как человек, направлены только две. Речь идет об идентификации и аутентификации пользователей и о разграничении доступа к информационным ресурсам. Электронная цифровая подпись является одним из методов идентификации пользователя, а также выполняет в документообороте важнейшую функцию подтверждения подлинности сведений, содержащихся в сообщении.

Рассмотрим более подробно категории «идентификация» и «аутентификация». Первый из указанных терминов этимологически образован от латинского слова identifico (отождествлять), и среди многочисленных случаев его применения в русском языке для рассматриваемого в данном исследовании случая наиболее правильным было бы использование слова «опознание». А. Ю. Щеглов и К. А. Щеглов полагают, что «идентификация – это процесс распознавания элемента системы, обычно с помощью заранее определенного идентификатора или другой уникальной информации»[1].

Категория «идентификация» также чрезвычайно широко используется в нормативных правовых актах различного уровня, но в большинстве случаев ее определение не осуществляется, так как термин, видимо, относится разработчиками данных актов к разряду общеупотребительных. Одно из исключений представляет собой Соглашение между Правительством Российской Федерации и Правительством Финляндской Республики о со-

[1] Щеглов А. Ю. Идентификация и аутентификация. Так ли все просто? // URL: www/npp-itb.ru

трудничестве и борьбе с преступностью[1], где приводится такое определение: «идентификация лица означает опознание лица, подозреваемого в совершении преступления, или жертвы несчастного случая на основе отпечатка пальцев, других признаков, фотоснимка или других сведений».

Таким образом, авторский коллектив может утверждать, что категория «идентификация» тождественна слову «опознание» и техническая система, реализуя процедуру идентификации, опознает субъекта, который желает получить доступ в систему для совершения каких-либо действий (в случае информационной системы – для ознакомления, копирования, модификации, блокирования либо уничтожения информации).

С категорией «аутентификация» дело обстоит несколько сложнее. Как следует, в частности, из положений Стандарта Банка России «Обеспечение информационной безопасности банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014»[2]:

- идентификация – процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов;

- аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности).

Таким образом, в целях упрощения понимания можно сказать: идентификация – это выдача пропуска с уникальным номером и проверка пропуска по номеру; аутентификация – сверка фотографии с лицом субъекта, предъявившего пропуск, и проверка, не переклеена ли фотография в подлинном пропуске.

На основании вышеизложенного можно утверждать, что, во-первых, аутентификация является функцией идентификации, а идентификация имеет техническую и юридическую составляющие. Последняя, юридическая составляющая, программой создания единой телекоммуникационной системы органов внутренних дел совершенно не учитывается. Но для эксплуатации более чем трех тысяч банков данных, существующих в органах внутренних дел, проблема определения полномочий сотрудников органов внутренних дел и иных лиц к содержанию этих банков данных имеет первостепенное значение, более важное, чем использование межсетевых экранов последней модификации.

Разработчикам Программы создания единой телекоммуникационной системы, а также всем иным должностным лицам, которые при подготовке

---

[1] Соглашение между Правительством Российской Федерации и Правительством Финляндской Республики о сотрудничестве и борьбе с преступностью : заключено в г. Москве 05.03.1993 // Бюллетень международных договоров. – 1997. – № 4. – С. 20–25.

[2] Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. СТО БР ИББС-1.0-2014» : распоряжение Банка России от 17.05.2014 № Р-399 // Вестник Банка России. – 2014. – № 48–49.

проектов нормативных правовых актов описывают содержание мероприятий по обеспечению защиты информации, необходимо прежде всего определиться, какой метод разграничения доступа они будут применять, осознавая, что в конечном итоге от этого зависит обеспечение целого ряда прав и свобод человека и гражданина, в том числе права на жизнь, достоинство личности и неприкосновенность частной жизни.

Анализ многочисленной литературы по вопросам обеспечения информационной безопасности[1] позволяет авторскому коллективу выделить несколько наиболее распространенных методов разграничения доступа к информационным ресурсам в банках данных:

- разграничение доступа к сведениям по спискам;
- использование матрицы установления полномочий обращения с информационными ресурсами;
- разграничение доступа по уровням конфиденциальности;
- парольное разграничение доступа.

Попробуем более детально разобраться в сущности этих методов, так как это, по мнению авторского коллектива, необходимо для совершенствования правового регулирования отношений в сфере использования банков данных органов внутренних дел.

Как предполагает авторский коллектив, существенный скачок в автоматизации процессов информационного обмена в органах внутренних дел, в которые неизбежно будут вовлечены и сведения конфиденциального характера, произойдет совсем скоро.

При этом, по мнению авторского коллектива, важно избежать исключительно технического подхода в обеспечении важнейшего из элементов обеспечения защиты информации в банках данных – разумного разграничения доступа.

Можно привести следующий пример исключительно технического подхода к решению данной проблемы в системе защиты информации VipNet, которая, кстати, стала активно внедряться в органах внутренних дел.

Как констатируется в курсе лекций «Система защиты информации VipNet», описывающем функционирование данной системы, «управление политиками безопасности осуществляется с помощью шаблонов, назначаемых управляемым узлам. Шаблон политики безопасности представляет собой именованный набор параметров безопасности и может содержать сетевые фильтры и правила трансляции IP-адресов. Для удобства управле-

[1] См., напр.: Грязнов Е., Панасенко С. Безопасность локальных сетей // Мир и безопасность. – 2013. – № 2.; Котухов М. М., Марков А. С. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности. Автоматизация систем. – М., 1998.

ния узлы можно объединять в подразделения и назначать шаблоны как отдельным узлам, так и подразделениям»[1].

Это означает, что возможна разработка любых моделей разграничения доступа и их автоматизированное внедрение в групповых или индивидуальных сегментах системы.

Однако разработка самих моделей является суверенной задачей эксплуатирующей организации. Пока в этом вопросе в органах внутренних дел в нормативных правовых актах присутствует существенная разноголосица, причем все более склоняющаяся к технократическому изложению нормативных предписаний.

Попробуем все же подойти к данному вопросу с точки зрения здравого смысла, базирующегося на фундаментальных положениях законодательства Российской Федерации. Модель оборота конфиденциальной информации в общем и целом представляет собой упрощенную модель оборота сведений, составляющих государственную тайну, где издавна применяется уровневый принцип разграничения доступа, основанный на степенях секретности информации. Но при этом каждый, кто сталкивается с государственной тайной, прекрасно знает, что одного только допуска к этим сведениям недостаточно – необходимо административное разрешение уполномоченного должностного лица на ознакомление с конкретной информацией в рамках общей степени секретности.

К сведениям конфиденциального характера в органах внутренних дел потенциально могут быть допущены все сотрудники и государственные гражданские служащие, так как специальной процедуры оформления допуска к этой информации не предусмотрено. Но это опять же не означает, что любой сотрудник вправе ознакомиться с любыми сведениями, которые содержатся в банках данных конфиденциальной информации, так как, получив сведения, он может запомнить эту информацию и сообщить ее заинтересованному лицу. Никакими техническими приемами данный процесс остановить не удастся. Остаются организационно-правовые методы. Их по сути два: установление из круга лиц, которые были ознакомлены с определенными сведениями, конкретного лица, которое передало информацию, и привлечение его к юридической ответственности.

В реализации упомянутого выше метода разграничения доступа по спискам существуют два подхода – либо для каждого пользователя определяется список информационных ресурсов, к которым он может быть допущен, либо для каждого информационного ресурса определяется список пользователей.

Для многочисленных банков данных органов внутренних дел должны применяться обе разновидности данного метода. Это влечет за собой

[1] Система защиты информации VipNet : курс лекций / под общ. ред. О. А. Чефрановой. – М., 2014. – С. 171.

решение достаточно масштабной, но необходимой задачи – установления для каждого банка данных основного способа разграничения в доступе к информации. Причем делать это придется на основе характеристик самих пользователей.

Авторский коллектив настоящего исследования не претендует на полное решение вышеуказанной задачи, однако можно сразу выделить две категории сотрудников, которые могут служить основными моделями – руководители и сотрудники оперативных подразделений. В свою очередь, руководители должны подразделяться на общих и руководителей структурных подразделений.

По мнению авторского коллектива, общие руководители (начальник органа внутренних дел и его заместители, начиная с уровня района) должны иметь доступ ко всем информационным ресурсам органов внутренних дел, в которых накапливается информация конфиденциального характера, в том числе к банкам данных, перечисленным в п. 3 ст. 17 Федерального закона «О полиции», за исключением сведений о лицах, в отношении которых заведены дела оперативного учета (п. 17), о лицах, прошедших государственную геномную регистрацию (п. 19), и о лицах, подлежащих государственной защите (п. 20).

Сведения о лицах, в отношении которых заведены дела оперативного учета, чаще всего подпадают под категорию государственной тайны, но даже если и не подпадают, то только подразделения, ведущие такую разработку, решают, кому, кроме прямых начальников, возможно сообщить данные сведения. Геномная регистрация является специфическим учетом, относящимся к категории биометрических персональных данных, и для него должны оговариваться отдельные условия доступа. К сведениям, связанным с мероприятиями, проводимыми в отношении лиц, подлежащих государственной защите, должно быть допущено минимальное число лиц, прямо связанных с реализацией указанных мероприятий. Соответственно, к таким банкам данных реализуется доступ по заранее определенному списку пользователей.

Следующий метод, связанный прежде всего с целостностью и достоверностью информации, – *метод матрицы установления полномочий*. Согласно этому методу в некоем формализованном списке определяется набор полномочий, которыми вправе обладать конкретный пользователь по отношению к определенным информационным ресурсам. Например, он вправе только знакомиться либо знакомиться и дополнять, знакомиться, дополнять и корректировать, копировать, удалять и т.д.

Данный формальный набор полномочий очень важен и должен быть тщательно продуман. Например, руководитель подразделения, который на самом деле в силу своих должностных полномочий принимает решения о модификации и удалении сведений из банка данных, не должен обладать

возможностью фактической реализации такого полномочия, а реализовывать свое волеизъявление через определенную процедуру дачи документально оформленного указания. Технологическими возможностями внесения данных изменений должен обладать администратор банка данных или специально определенный пользователь.

Следующим из обычно выделяемых методов разграничения в доступе является *разграничение по уровням конфиденциальности (категориям)*.

Данный метод хорошо работает при формальном разделении информации по степеням секретности в системе отнесения сведений к государственной тайне. Но даже там он слишком схематичен, так как массивы информации, отнесенные к той или иной степени секретности (за исключением сведений категории «особой важности»), являются достаточно большими и разнородными по содержанию.

Приведем пояснительный пример. К сведениям, раскрывающим личность гражданина, установившего конфиденциальное сотрудничество с органами внутренних дел, имеют доступ не все лица, имеющие допуск к совершенно секретной информации, а только немногочисленный, строго ограниченный круг сотрудников.

Поэтому в подавляющем большинстве банков данных полиции можно выделить некоторые локальные сегменты, которые необходимо охранять наиболее тщательно, детально регламентируя порядок доступа, круг лиц, порядок фиксации фактов обращений к содержанию сегмента банка данных и т.п.

Например, среди так называемых «гражданских» номеров автотранспортных средств есть серии, закрепленные за закрытыми административными ведомствами, и к сведениям о конкретном распределении таких номеров не должно быть общего доступа.

Последний из обычно выделяемых методов разграничения – *парольный*. Его также можно назвать интегративным по отношению ко всем описанным выше, так как именно в пароль можно заложить как общее полномочие доступа, так и матричное, а также категориальное.

Парольная система универсальна, однако у нее есть один существенный изъян – содержание пароля может стать известным неуправомоченному субъекту и этот неуправомоченный субъект может длительное время получать доступ к сведениям, находящимся в том или ином банке данных, скрытно.

Для этих целей в современных автоматизированных информационных системах применяется такой метод защиты, как ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя. Суть этого метода заключается в фиксации попытки получения доступа в систему под теми же учетными данными (паролем) в тот момент, когда такой доступ имеет легальный пользователь, и блокировании второго процесса.

Но все описанное выше – только технология, за которой должны последовать определенные правовые действия: блокирование ключа легального пользователя, назначение расследования по факту утечки информации и определение объемов сведений, к которым был осуществлен несанкционированный доступ, генерация (изготовление) нового ключа для легального пользователя и т.д.

Такая административная процедура должна быть предметом нормативных правовых актов, регулирующих вопросы защиты информации в органах внутренних дел, однако в результате изучения массива данных актов авторский коллектив настоящего исследования регламентации этих вопросов не обнаружил.

В описанном выше случае наиболее опасным является удаленный доступ, который осуществляется из мест, находящихся за пределами так называемой контролируемой зоны, то есть фактически за пределами административного здания, в котором расположено компьютерное оборудование, содержащее банк (или банки) данных. Всего существуют две принципиальные модели организации удаленного доступа к автоматизированным банкам данных – по выделенным каналам связи и по каналам связи общего пользования.

В случае организации доступа по выделенным, а еще лучше – защищенным каналам связи, проблема несанкционированного доступа скорее всего будет сведена к обычной технической ошибке, так как круг лиц, которые имеют доступ к выделенному защищенному каналу связи, изначально ограничен. Однако в эпоху мобильной связи и Интернета попытка организовать доступ только через кабельные сети обречена на провал. Выделенные защищенные каналы в настоящее время хороши только между стационарными крупными объектами, например, между административными зданиями, в которых расположены подразделения одного органа внутренних дел, расположенными в одном населенном пункте.

Время же диктует нам, причем диктует настоятельно, развитие именно удаленного мобильного доступа, позволяющего уполномоченным сотрудникам получить доступ к банкам данных непосредственно с места проведения оперативно-следственных действий, с места выполнения служебного задания и т.п.

Именно реализация данного подхода, когда в единицу времени уполномоченный сотрудник может получить максимум необходимой для анализа и принятия решения информации, приводит к перспективе достижения должного служебного результата меньшими силами, удешевления содержания административного аппарата, повышению качества и результативности работы.

Авторский коллектив понимает что проблема упорядочения оборота сведений конфиденциального характера в органах внутренних дел является одним из звеньев в общей цепочке их деятельности, в которой все

большее значение приобретает автоматизация процессов оперативно-служебной деятельности.

Среди нормативных правовых актов, имеющих для перспектив деятельности органов внутренних дел долговременный и системный характер, является Приказ МВД России от 14.10.2011 № 1070 «Об утверждении ведомственного плана МВД России по повышению эффективности бюджетных расходов», в одном из положений которого говорится следующее:

«Исторически сложившееся организационное построение органов внутренних дел базируется на административно-территориальных и линейных принципах обслуживания населения.

Действующая система не соответствует концептуальным основам административной реформы и современным моделям организационного построения федеральных органов исполнительной власти. Полиция, являющаяся неотъемлемой и основной частью органов внутренних дел Российской Федерации, не обладает организационным единством, базируется на принципах тройного подчинения (Министерству внутренних дел, региональным органам власти и органам местного самоуправления)».

Первым следствием данного анализа явилось решение о сокращении общей штатной численности органов внутренних дел на 20%, которое должно было компенсироваться модернизацией деятельности по целому ряду направлений. Среди таких направлений данный приказ, в частности, выделил создание единого информационного пространства органов внутренних дел, создание электронных оперативно-справочных карточек, в которых на момент подписания приказа числилось 75,5 млн единиц учетных документов, касающихся осужденных, привлеченных к уголовной ответственности и разыскиваемых лиц.

При этом констатировалось, что доступ правоохранительных органов к электронным информационным ресурсам автоматизированных картотек будет осуществляться с использованием современных информационно-телекоммуникационных технологий по каналам связи Единой интегрированной информационно-телекоммуникационной системы органов внутренних дел. Это позволит обеспечить оперативность и качество проверки лиц, задержанных по подозрению в совершении преступлений и правонарушений, раскрытия преступлений «по горячим следам», а также пресечения преступлений на стадии приготовления к покушению.

Одним из способов технической реализации таких перспектив стала ведомственная система электронной почты «Дионис», которая функционирует в интегрированной мультисервисной телекоммуникационной системе МВД России.

Следует отметить, что данная система стала активно внедряться в органы внутренних дел, в особенности на уровне МВД (ГУВД) региона – районный орган внутренних дел. Рассмотрим некоторые аспекты функци-

онирования данной системы на примере МВД России по Удмуртской республике. Как констатируется в Приказе МВД России по Удмуртской республике от 03.04.2006 № 266, ведомственная магистральная сеть передачи данных «Дионис» является системой, обеспечивающей передачу несекретных данных по магистральным каналам от звена «МВД России» до звена «отдел внутренних дел по административному району».

При этом приказ не раскрывает понятия «несекретные данные». Как полагает авторский коллектив, не имеет смысла создавать какую-либо информационно-телекоммуникационную систему ведомственного уровня, если она не допускает возможности без дополнительных условий передачи хотя бы конфиденциальной информации служебного характера. Поэтому является довольно странным подход к определению уровня значимости сведений, представленный в вышеуказанном приказе.

Понятно, что данному ведомственному нормативному правовому акту около десяти лет и с того периода многое изменилось. Однако эта проблема для органов внутренних дел имеет куда более глубокие корни, чем кажется.

Многие ведомственные системы связи, которые в трансформированном виде действуют и сейчас, в нашей стране стали создаваться еще в советский период и продолжают совершенствоваться в настоящее время. К ним, в частности, относятся системы ведомственной связи Вооруженных Сил и органов безопасности, которые обеспечивают не только бесперебойность, но и известную конфиденциальность передаваемой информации.

Органы внутренних дел в силу их разветвленности и территориальной привязки к единицам административного деления изначально опирались на сети связи общего пользования, которые создавало и поддерживало Министерство связи. Защиту сведений, составляющих государственную тайну, при передаче информации по каналам связи обеспечивала шифровальная служба, остальная информация передавалась по телефонным и телеграфным абонентским системам связи без какой-либо дополнительной защиты.

Канальная ведомственная привязка (то есть монопольное владение физической линией связи) оправдана по финансовым затратам только в случае постоянной передачи больших объемов информации (загрузки канала). В органах внутренних дел в подавляющем большинстве случаев загрузка каналов эпизодическая, что делает приобретение в собственность или аренду линий связи во многих случаях экономически невыгодными.

Новые технологические реалии, связанные с компьютеризированной обработкой и передачей сведений, свидетельствуют о том, что современные информационно-телекоммуникационные системы вполне могут опираться на физические линии связи общего пользования и в то же время формировать собственные сети передачи информации с любым уровнем

защиты. Причем эти системы могут быть полисегментными, состоящими из подсистем разного предназначения.

По мнению авторского коллектива, именно эта техническая идеология и была заложена в создаваемую на протяжении многих лет Единую информационно-телекоммуникационную систему органов внутренних дел (ЕИТКС). Одним из сегментов ЕИТКС и явилась система «Дионис», которая по имеющимся у авторского коллектива сведениям представляет собой разветвленную сеть почтовых серверов сети Интернет, полностью контролируемых органами внутренних дел.

Использование системы электронной почты ныне стало повседневной реальностью. Практически каждый интернет-пользователь имеет электронный почтовый ящик, отправляет и получает текстовые и графические изображения. Говоря иначе, такая система коммуникаций давно стала повседневной реальностью, вобрав в себя в том числе значительную часть деловой переписки. Электронные письма в целом ряде случаев стали признаваться судами в качестве доказательств.

С точки зрения обеспечения защиты информации в системе публичной электронной почты имеется один существенный изъян – пользователь не знает, на каком сервере физически хранится его информация и кто может к ней иметь технический доступ. Парольная защита, которой обеспечен каждый электронный почтовый ящик, направлена против попыток проникновения извне, но не против открытия доступа к содержанию информационного ресурса со стороны владельцев сервера, которые в любом случае в состоянии организовать технологический доступ к содержанию почтового ящика.

Поэтому формирование системы, где почтовые серверы находятся в техническом обслуживании органов внутренних дел, явилось в свое время абсолютно правильным организационным решением.

Как представляется авторскому коллективу, формирование новой коммуникационной среды должно было привести к обеспечению возможности любому сотруднику стать обладателем персонального почтового ящика, однако этого обеспечено не было. Из контекста рассматриваемого приказа МВД России по Удмуртской республике следует, что на каждый районный орган внутренних дел должна приходиться только одна рабочая станция системы «Дионис», к которой возможно подключение других рабочих станций по локальной сети. Такой подход резко снижает возможности информационного обмена.

Помимо всего вышесказанного, для системы «Дионис», равно как и для любой иной системы обмена электронными сообщениями, существует проблема подтверждения подлинности отправленного сообщения, что сводится к двум основным моментам, имеющим правовое значение, а именно:

- к исключению возможности незаметного внесения изменений в текст сообщения;

- наличию свидетельства о том, что данный текст действительно исходит от конкретного сотрудника.

Данная проблема разрешается посредством применения электронной цифровой подписи (в соответствии с последними законодательными установлениями – электронной подписи). К моменту ввода в эксплуатацию системы «Дионис» нормативные условия для использования ЭЦП в нашей стране были уже созданы (Федеральный закон «Об электронной цифровой подписи»[1]), однако данная система при организации работ по эксплуатации сети «Дионис» нигде не упоминается.

Изучение иных материалов, относящихся в том числе к сети «Дионис», показало, что она изначально строилась как предназначенная только для передачи сведений, не имеющих никаких ограничительных пометок. Об этом, в частности, свидетельствует проведенный авторским коллективом анализ Методических рекомендаций по использованию Единой информационно-телекоммуникационной системы органов внутренних дел, разработанных ИЦ МВД России по республике Дагестан в 2011 г. В этом документе прямо содержится запрет для пользователя электронной почты «Дионис» использовать и обрабатывать почтовую конфиденциальную информацию и сведения, составляющие государственную тайну, а в случае получения такой информации от других лиц пользователь обязан сообщить о данном факте непосредственному начальнику для последующего уведомления подразделения режима и информационной безопасности.

По мнению авторского коллектива, формирование интегрированной многоуровневой системы, которая реально охватила бы все органы внутренних дел, исключительно для передачи общедоступных сведений является неоправданным расточительным решением.

Теперь авторский коллектив хотел бы обратиться к анализу еще ряда ведомственных нормативных правовых актов, которые в той или иной степени связаны с проблемой осуществления оборота сведений конфиденциального характера в органах внутренних дел.

Общеизвестно, что одним из самых экономически оправданных способов (методов) защиты информации при ее передаче с помощью технических средств связи является криптографическое преобразование. Как отмечает С. Сингх, «тысячи лет короли, королевы и полководцы управляли своими странами и командовали своими армиями, опираясь на надежно и эффективно действующую связь. В то же время все они осознавали последствия того, что произойдет, если их сообщения попадут не в те руки, если вражескому государству будут выданы ценные секреты, а жизненно

[1] Об электронной цифровой подписи : федеральный закон от 06.04.2011 № 63-ФЗ // СПС «Консультант Плюс».

важная информация окажется у противника. И именно опасение того, что враги перехватят сообщение, послужило причиной активного развития кодов и шифров – способов скрытия содержания сообщения таким образом, чтобы прочитать его смог только тот, кому оно адресовано»[1].

Опускаясь с высоты прошлых исторических эпох на почву современной обыденности, авторский коллектив отмечает, что криптографическое преобразование информации при правильной организации защищенного информационного обмена позволяет решить ряд важных юридических задач:

1) обеспечить передачу информации от отправителя к получателю в точном соответствии с первоначальным текстом;

2) обеспечить прочтение информации только тем лицом, которому оно адресовано;

3) обеспечить регистрацию факта каждого получения лицом определенного объема сведений (фиксацию факта ознакомления), что имеет ключевое значение для определения круга подозреваемых в случае утечки информации и доказательства вины конкретного лица.

Криптографическое преобразование информации использовалось органами внутренних дел для защиты передаваемых сведений еще в имперский период существования нашего государства, о чем свидетельствуют многочисленные документы, сконцентрированные в фонде № 102 Государственного архива Российской Федерации, и материалы работы Т. А. Соболевой «История шифровального дела в России»[2].

Практически весь советский и современный нам период криптографические средства использовались и используются в органах внутренних дел для защиты сведений, составляющих государственную тайну. Об этом в том числе свидетельствует изложенная в Концепции развития системы криптографической защиты информации в органах внутренних дел до 2013 года, утвержденной Приказом МВД России от 02.08.2010 № 561, констатация следующих фактов:

«Подсистема обеспечения криптографической защиты сведений, составляющих государственную тайну, в органах внутренних дел не является полномасштабной и не обеспечивает современные потребности органов внутренних дел в передаче сведений ограниченного доступа по каналам связи, что создает предпосылки для передачи сведений ограниченного доступа по каналам связи в незащищенном виде.

Проблемы в обеспечении органов внутренних дел шифрованной связью сложились на районном уровне территориальных органов МВД России. Основными негативными факторами на указанном уровне управления МВД России являются:

---

[1] Сингх С. Книга шифров. Тайна история шифров и их расшифровки. – М., 2007. – С. 9.

[2] Соболева Т. А. История шифровального дела в России. – М. : ОХМА-ПРЕСС, 2002 .

- низкий уровень организации шифровальной службы на региональном уровне управления органами внутренних дел, не обеспечивающий полномасштабное использование шифрованной связи на районном уровне;

- использование для криптографической защиты сведений, составляющих государственную тайну, шифровальной техники, реализованной на устаревшей технологической базе, либо трудоемких ручных средств шифрования».

Упоминание в данном акте категории «ручные средства шифрования», по мнению авторского коллектива, является весьма символичным. Под ними понимаются способы преобразования информации путем замены букв, слов, а иногда типовых фраз на условные обозначения, чаще всего группы цифр, последовательность которых затем передается по каналам связи. Такая замена осуществляется непосредственно физическим лицом на основе каталога условных обозначений, именуемого в криптографии кодом, а этот процесс называется ручным шифрованием.

Подобные системы шифрования применялись еще в XIX веке и упоминание о них в веке XXI говорит о том, что в вопросах применения средств криптографической защиты информации органы внутренних дел действительно отстали от технологического прогресса, когда шифрование информации стало делом компьютерных технологий и существуют тысячи различных программ и аппаратно-программных комплексов, решающих такие задачи на обыкновенном персональном компьютере.

При этом концепция фиксирует и ряд других негативных явлений. Так, в частности, констатируется следующее:

«Существующие информационно-телекоммуникационные системы ОВД и создаваемая интегрированная мультисервисная телекоммуникационная система ОВД не обеспечивают выполнения требований информационной безопасности по защите конфиденциальной информации, содержащей служебные сведения и персональные данные граждан.

Полномасштабная система органов криптографической защиты информации с функциями разработки и практического осуществления мероприятий по обеспечению безопасности хранения, обработки и передачи конфиденциальной информации по каналам связи с использованием СКЗИ, в том числе по обеспечению юридической значимости электронного документооборота с использованием средств ЭЦП, в системе МВД России не создана.

Негативными факторами, затрудняющими реализацию мероприятий по данному направлению, являются:

- отсутствие ведомственной нормативной правовой базы, отвечающей современным требованиям по информационной безопасности;

- отсутствие квалифицированных специалистов в области защиты конфиденциальной информации с применением средств криптографической защиты информации, в том числе средств ЭЦП».

Приведенные положения прежде всего содержат свидетельство о том, что интегрированная телекоммуникационная система органов внутренних дел создавалась без учета реализации задач гарантированной защиты информации.

Не создана также управляющая система, то есть система подразделений, на которые возложена задача организации криптографической защиты информации в органах внутренних дел.

Следует обратить внимание на тот факт, что в рамках общей цели криптографической защиты информации обозначена задача «по обеспечению юридической значимости электронного документооборота с использованием средств ЭЦП».

Авторский коллектив может констатировать, что задача подтверждения подлинности информации посредством электронной подписи есть частный случай общей задачи криптозащиты информации и имеет смысл в рамках данного раздела исследования на нем хотя бы вкратце остановиться.

Проблема оборота сведений в электронной форме отображения является одной из важных задач, которые должны решаться в общей системе государственного управления. Перевод документов в электронную форму имеет целый ряд неоспоримых преимуществ, так как резко уменьшает затраты на хранение документов, существенно облегчает поиск документов и определенной информации в них, позволяет осуществлять различные классификации, группировать документы в банках данных и т.п.

При всех неоспоримых преимуществах электронный документ в сравнении с документом на традиционном бумажном носителе обладает одним весьма существенным недостатком – его содержание может быть незаметно изменено, а фиксация подписи соответствующего руководителя в таком документе представляет собой известную сложность.

Именно на решение данной задачи и направлена электронная подпись, которая одновременно является математическим криптографическим алгоритмом, реализованным в определенной компьютерной программе, и юридической категорией.

Система электронной подписи позволяет одновременно четко сопоставить ее с конкретным физическим лицом (аналог собственноручной подписи) и не менее четко указать, изменялось содержание документа после его подписания электронной подписью либо нет.

Поэтому задача простого перевода документов в электронную форму не является полным решением проблем автоматизации электронного документооборота – необходимо совместно с каждым документом сохранять

электронную подпись подписавшего его должностного лица, а также сертификат ключа проверки электронной подписи.

В органах внутренних дел традиционно сложилась определенная система, согласно которой только некоторые должностные лица имеют право подписи документов, направляемых за пределы конкретного подразделения. Это, как правило, руководитель подразделения и его заместители. Еще меньшее число должностных лиц вправе направлять за своей подписью документы в вышестоящие органы внутренних дел или иные органы государственной власти.

Система ведомственной организации электронного документооборота с использованием электронных подписей должна учитывать вышеуказанное обстоятельство, а также тот факт, что помимо лица, подписывающего документ, есть лицо, исполняющее документ, то есть подготавливающее его. Оно тоже должно нести ответственность за его содержание. Помимо них есть лица, которые визируют документ, то есть выражают свое согласие с его содержанием до того момента, когда он будет подписан основным должностным лицом. Их электронные подписи также имеют существенное значение при установлении юридической значимости документа.

Отсюда напрашивается вывод о том, что система ведомственного документооборота с использованием электронных подписей должна выстраиваться по аналогии с системой бумажного документооборота и подразделения криптографической защиты здесь ни при чем.

Данная логика очевидна, но имеет один нюанс – в соответствии с нормами Федерального закона «Об электронной подписи»[1] средства электронной подписи – это шифровальные (криптографические) средства, используемые для реализации одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Отсюда следует, что принятие решения о том, кому предоставлять возможность подписывать электронные документы, – это дело руководства органа внутренних дел и подразделений делопроизводства, а установка средств электронной подписи и контроля за их работоспособностью – задача подразделений, занимающихся криптографической защитой информации.

Это привело авторский коллектив к необходимости анализа организационной структуры подразделений по защите информации.

Как следует из данных, размещенных на сайте МВД России (www.mvd.ru), в структуре министерства действует Департамент информационных технологий, связи и защиты информации, положение о котором утверждено Приказом МВД России от 16.06.2011 № 681. Данный департамент подчинен заместителю Министра внутренних дел, ответственному за

[1] Об электронной подписи : федеральный закон от 06.04.2011 № 63-ФЗ // СПС «Консультант Плюс».

блок материально-технического и медицинского обеспечения министерства (приказ МВД России от 12.07.2012 № 690).

Среди основных задач, которые возлагаются на департамент, значится организация обеспечения мероприятий по технической (в том числе криптографической) защите государственной тайны и информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

В свою очередь, среди основных функций и полномочий, которые реализует департамент, имеется функция «организации шифровальной службы в органах, организациях и подразделениях системы МВД России, руководство деятельностью шифровальных органов и органов криптографической защиты информации по специальным вопросам и контроль за ней».

Из данного положения следует, что в органах внутренних дел все же отдельно действуют шифровальные органы и органы криптографической защиты информации, и можно предположить, что первые обеспечивают защиту сведений, составляющих государственную тайну, а вторые по логике должны быть ответственны за защиту сведений конфиденциального характера.

Приказом МВД России от 02.07.2012 № 660 утверждено Типовое положение о подразделении информационных технологий, связи и защиты информации территориального органа Министерства внутренних дел Российской Федерации. Среди пяти основных задач, поставленных перед данными подразделениями, две задачи прямо касаются защиты информации:

- организация и реализация мероприятий по противодействию технической разведке и технической (в том числе криптографической) защите информации;

- обеспечение функционирования и безопасности шифрованной связи в территориальном органе.

Пять основных задач трансформируются в тридцать восемь основных функций подразделений информационных технологий, связи и защиты информации, среди которых вопросы собственно защиты информации занимают уже существенно более скромное место на фоне остальных задач.

Оставив за скобками вопросы организации шифровальной службы, можно выделить три задачи, которые охватываются предметом настоящего исследования:

- осуществление мероприятий по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, защите персональных данных при автоматизированной обработке и контроле за их проведением подразделениями территориального органа;

- осуществление мероприятий по противодействию техническим разведкам; радиоэлектронной борьбе; технической (криптографической) защите информации;

- осуществление контроля за обеспечением в подразделениях территориального органа исполнения предписаний нормативных правовых актов в области защиты информации.

Первичный анализ данных положений показывает формальное существование системы подразделений, на которые возложена задача защиты конфиденциальной информации, в том числе персональных данных, однако эта важная функция значится одной из десятков других задач и функций, и не факт, что ей будет уделяться должное внимание и выделяться должное ресурсное обеспечение как приоритетной задаче.

Система организации защиты информации в органах внутренних дел ныне построена схематично следующим образом:

- информация на бумажных носителях – подразделения делопроизводства и режима;

- информация в автоматизированных системах и при передаче по каналам связи – подразделения информационных технологий, связи и защиты информации.

Эти службы имеют различное подчинение: первые – непосредственно руководителю органа внутренних дел, вторые – одному из его заместителей. Уже в этом есть определенный дисбаланс. Но самый основной недостаток, в том числе порождающий те проблемы, о которых авторский коллектив говорил и в данном, и в предшествующих параграфах исследования, – это отсутствие «единого мозгового центра», обособленного подразделения, на которое должна быть возложена задача выработки политики организации защиты всей информации ограниченного доступа в органах внутренних дел и обеспечение контроля за исполнением нормативных предписаний.

Авторский коллектив предложил бы назвать данное подразделение на уровне МВД России управлением по защите информации и подчинить непосредственно Министру внутренних дел. Подчиненность первому руководителю обусловлена прежде всего тем, что данные проблемы не будут рассматриваться как второстепенные, равные среди прочих. Именно такая подчиненность, по имеющимся у авторского коллектива сведениям, существовала в отношении шифровальной службы органов внутренних дел в советский период и первые годы существования современного российского государства и доказала свою состоятельность.

Данное подразделение, по мнению авторского коллектива, должно осуществлять не только выработку ведомственной политики по защите информации ограниченного доступа, но и осуществлять комплекс таких мероприятий, объединив в своей структуре и подразделения, реализующие организационные функции, и подразделения, осуществляющие контроль, и подразделения, осуществляющие проведение технических мероприятий.

Только при реализации вышеописанного подхода будет достигнут должный эффект в реальном осуществлении защиты конфиденциальной информации в органах внутренних дел.

В качестве заключения к данному параграфу исследования авторский коллектив хотел бы отметить следующее:

1. Проведенный авторским коллективом анализ показал, что важнейшим методом упорядочения доступа к информационным ресурсам органов внутренних дел в виде банков данных является метод идентификации и аутентификации пользователей, который имеет техническую и юридическую составляющие. В подавляющем большинстве нормативных актов делается упор на техническую составляющую, оставляя приобретение конкретного объема правомочий по доступу к информации (юридическая составляющая) для административного усмотрения конкретных руководителей, которые, к сожалению, могут и не обладать должным уровнем знаний и компетенции в вопросах разграничения полномочий между подчиненными сотрудниками и иными потенциальными пользователями.

Какого-либо акта МВД России, который устанавливал бы централизованно принципы и условия применения методов разграничения доступа к информационным ресурсам, содержащим сведения конфиденциального характера, до сего времени не принято. В данном акте, помимо указанного, должны быть детально описаны процедуры, следующие за обнаружением факта попытки несанкционированного доступа к информационным ресурсам органов внутренних дел и прежде всего к банкам данных полиции.

Это особенно актуально в условиях повсеместного внедрения технологий удаленного мобильного доступа к информационным ресурсам.

2. Если предположить, что технологии удаленного и особенно мобильного доступа к информационным ресурсам органов внутренних дел будут активно развиваться, то на первый план в вопросах защиты информации выходит не только проблема упорядочения доступа, но и проблема защиты информации при ее передаче по каналам связи. Эта защита должна осуществляться не только в целях сохранения целостности передаваемых сведений, но и предусматривать исключение ознакомления с ней в случае непреднамеренного или преднамеренного попадания к третьим лицам. В условиях полной компьютеризации систем передачи данных это не банальный перехват в радиоэфире, а возможность параллельного перенаправления сведений за счет использования специальных программ.

Отсюда следует, что в органах внутренних дел должны активно развиваться технологии криптографической защиты информации при ее передаче по техническим каналам связи, в том числе и при использовании глобальных информационно-телекоммуникационных систем.

§ 5. Административная ответственность в области защиты информации конфиденциального характера и юрисдикционные полномочия органов внутренних дел в данной сфере

Является общеизвестным теоретическое положение о том, что юридическое обязывание или юридический запрет только тогда действенны, если они подкреплены угрозой наказания за их нарушение.

Применительно к рассматриваемой в рамках настоящего исследования проблематике следует отметить, что вполне возможно однозначно установить наличие взаимозависимости между уровнем четкости правового регулирования отношений в сфере оборота сведений, составляющих государственную тайну, а также их соблюдения, с одной стороны, и жесткостью юридических санкций за противоправные действия в отношении данной информации, с другой стороны.

Проведенный авторским коллективом анализ содержания Особенной части КоАП РФ показал, что к регулированию отношений в сфере конфиденциальной информации наиболее непосредственное отношение имеют четыре блока норм, объединенных в статьи 13.11 «Нарушение установленного порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)», 13.14 «Разглашение информации с ограниченным доступом», ч. 1 статьи 13.28 в части нарушения порядка предоставления информации о деятельности государственных органов и органов местного самоуправления, содержащей сведения, относящиеся к информации ограниченного доступа, и 17.13 «Разглашение сведений о мерах безопасности».

Подвергнем данные правоположения более детальному анализу. Статья 13.14 вне всякого сомнения является в указанном блоке норм центральной, так как охватывает весьма значительный спектр отношений в сфере защиты информации и в этом смысле является своего рода универсальной санкцией. Диспозиция данной административно-деликтной нормы изложена в КоАП следующим образом:

«Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, за исключением случаев, предусмотренных частью 1 статьи 14.33 настоящего Кодекса».

При внешней простоте изложения текст данного правоположения требует дополнительных и, по мнению авторов, существенных пояснений.

Начнем с изложения центрального наказуемого действия – разглашения. Данное понятие как юридическая категория исторически пришло в КоАП из уголовного законодательства, где оно традиционно используется

по отношению к сведениям, образующим государственную тайну, тайну усыновления и тайну предварительного расследования.

Лингвистически понятие «разглашение» производно от глагола «разгласить», который в Толковом словаре русского языка определяется следующим образом:

«Рассказав, сделать известным всем (то, что должно сохраняться в секрете). Всем, повсюду объявить, рассказать о чем-нибудь, распространить что-нибудь (какое-нибудь вздорное сообщение, нелепый слух и т.п.)»[1]

Мы видим, что в лингвистическом истолковании данного понятия заложены два способа совершения такого акта – устное сообщение либо иное распространение. Причем в обоих случаях оно обращено к неопределенному кругу лиц (сделать известным всем).

Отсутствие в УК РФ и КоАП РФ специальных дефиниций, описывающих содержание категории «разглашение», свидетельствует о том, что законодатель опирается на общее лингвистическое его истолкование. Однако комментаторы УК РФ, а следом за ними и судебная практика воспринимают данную категорию несколько иначе. Наиболее близким к лингвистическому истолкованию рассматриваемой категории применительно к статье 283 УК РФ является ее объяснение в «Комментарии к Уголовному кодексу Российской Федерации» под ред. В. М. Лебедева, где под разглашением сведений, составляющих государственную тайну, «следует понимать противоправное предание огласке этих сведений, в результате чего они стали достоянием других лиц» [2].

В данном случае авторский коллектив настоящего исследования рассматривает сочетание понятий «разглашение» и «предание огласке» как не более чем игру слов.

Другие комментаторы пытаются детализовать данное действие. Например, в «Комментарии к Уголовному кодексу Российской Федерации» под ред. А. В. Бриллиантова указано, что «с объективной стороны преступление состоит в таком разглашении сведений, составляющих государственную тайну, при котором они стали известны другим лицам. Под разглашением следует понимать предание огласке или распространение данных сведений с нарушением установленного порядка. Само разглашение может иметь форму как активных действий (сообщение в доверительной беседе; демонстрирование документов, схем, устройств и т.п.; открытый доклад или лекция; публикация в средствах массовой информации или печатных изданиях и др.), так и бездействия (непринятие мер для засекречивания перевозки соответствующих материалов; допущение посторонних к ознакомлению

[1] Толковый словарь русского языка / сост. С. И. Ожегов. – М., 1956. – С. 591.

[2] Комментарий к Уголовному кодексу Российской Федерации / отв. ред. В. М. Лебедев. – М., 2013. – С. 630.

с секретными сведениями и т.д.). Способ разглашения может быть любым: устно, письменно, с использованием средств массовой информации и т.д.» [1].

Здесь уже можно наблюдать более широкое истолкование рассматриваемого понятия, в некоторых аспектах противоречащее лингвистическому пониманию данного действия.

Следует отметить, что именно такой подход воспринял законодатель, формулируя категорию «разглашение информации, составляющей коммерческую тайну», изложенную в статье 3 Федерального закона «О коммерческой тайне», под которой понимается «действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору».

У авторского коллектива отсутствует уверенность в том, что данную дефиницию возможно применять по методу аналогии закона для регулирования административно-деликтных отношений, поэтому сам собой напрашивается вывод о том, что в примечании к статье 13.14 КоАП РФ целесообразно сформулировать соответствующее понятие.

Однако, по мнению авторского коллектива, от термина «разглашение» следует отказаться, заменив его категорией «противоправное распространение» как более точно отражающей сущность наказуемого действия. И ни в коем случае нельзя использовать понятие «противоправное распространение» как бездействие. Разглашение бездействием с точки зрения русского языка абсурдно.

Продолжим рассмотрение диспозиции статьи 13.14 КоАП РФ. Обратим внимание на тот факт, что законодатель до сего времени сохраняет в названии данной статьи категорию «информация с ограниченным доступом», которая, напомним, не фигурирует в ныне действующем Федеральном законе «Об информации, информационных технологиях и о защите информации», замененная расплывчатым понятием «конфиденциальность информации».

В диспозиции данной нормы использована иная юридическая формула – «информация, доступ к которой ограничен федеральным законом», то есть любая информация (сведения), в отношении которой установлен ограниченный оборот. В результате мы получаем весь спектр систем ограничения в доступе к информации – от государственной тайны до инсайдерских сведений – в виде одного состава административного правонарушения.

---

[1] Комментарий к Уголовному кодексу Российской Федерации : в 2 т. / под ред. А. В. Бриллиантова. – М. – 2015. – С. 434.

Оговорка в диспозиции «за исключением случаев, если разглашение такой информации влечет уголовную ответственность», по мнению авторского коллектива, говорит не о системном, а о процессуальном разграничении – в тех случаях, когда противоправное распространение сведений подпадает под действие уголовного законодательства, невозможно привлечение к административной ответственности по данной статье КоАП РФ.

Таких случаев авторский коллектив выделяет семь:

1) статья 147 (разглашение без согласия автора или заявителя сущности изобретения, полезной модели или промышленного образца до официальной публикации о них);

2) статья 155 (разглашение тайны усыновления (удочерения) вопреки воле усыновителя, совершенное лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну, либо иным лицом из корыстных или иных побуждений);

3) часть 2 статьи 183 (незаконные разглашение или использование сведений, составляющих коммерческую тайну, налоговую тайну или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе);

4) статья 283 (разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе, работе, учебе или в иных случаях, предусмотренных законодательством Российской Федерации, если эти сведения стали достоянием других лиц);

5) статья 310 (разглашение данных предварительного расследования лицом, предупрежденным в установленном законом порядке о недопустимости их разглашения, если оно совершено без согласия следователя или лицом, производящим дознание;

6) статья 311 (разглашение сведений о мерах безопасности, применяемых в отношении судьи, присяжного заседателя или иного лица, участвующего в отправлении правосудия, судебного пристава, судебного исполнителя, потерпевшего, свидетеля, других участников уголовного процесса, а равно в отношении их близких, если это деяние совершено лицом, которому эти сведения были доверены или стали известны в связи с его служебной деятельностью);

7) статья 320 (разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа, а также его близких, если это деяние совершено в целях воспрепятствования его служебной деятельности).

В настоящее время остается дискуссионным вопрос о том, возможно ли в случае прекращения уголовного преследования в отношении лица по одной или нескольким из перечисленных статей УК РФ привлечение его за то же деяние по статье 13.14 КоАП РФ.

Следует также обратить внимание на тот факт, что субъект данного административного правонарушения специальный – лицо, получившее доступ к этой информации в связи с исполнением служебных или профессиональных обязанностей.

Помимо указанного, имеется еще одно ограничение – действия рассматриваемой нормы не распространяются на случаи, когда речь идет о недобросовестной конкуренции. Говоря иначе, если действия лица, заключающиеся в разглашении информации, квалифицированы как недобросовестная конкуренция, то данное лицо должно быть привлечено к ответственности за недобросовестную конкуренцию.

Казалось бы, налицо универсальная административно-правовая санкция, которая является действенным препятствием на пути противоправного распространения конфиденциальной информации.

Однако, во-первых, во многих случаях следует серьезно потрудиться, чтобы обосновать, что перед нами именно служебная информация ограниченного распространения, то есть, например, сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с регистрацией акта гражданского состояния, сведения, относящиеся к процедуре медиации, или что-то иное. Во многих случаях, к сожалению (и авторский коллектив настоящего исследования надеется, что он это убедительно доказал), весьма затруднительно квалифицировать принадлежность определенной информации к категории конфиденциальной. Не менее сложно при отсутствии единой легальной дефиниции квалифицировать то или иное деяние именно как разглашение.

Теперь поднимем один из самых существенных, если не основной для рассматриваемой статьи вопрос: а ради чего применяются юридические санкции? Величина наказания в статье 13.14 КоАП РФ настолько мизерна, что всякая доктринальная суета по этому поводу выглядит неосновательной – гражданин или должностное лицо, например, за сведения об абонентах или оказываемых им услугах связи (статья 53 Федерального закона «О связи»[1]) подлежат: первый – штрафу в размере от 500 до 1000 рублей, второй – от 4000 до 5000 рублей.

Данный подход законодателя говорит о том, что он слабо заинтересован в реальной защите конфиденциальной информации от противоправного распространения, если все ее многочисленные разновидности защищаются безо всякой дифференциации слабой штрафной санкцией.

Теперь обратимся к процессуальной составляющей данной проблемы. Начать административное преследование за рассматриваемое правонарушение, как следует из норм главы 28 КоАП РФ, вправе два вида субъектов – прокурор и должностные лица органов внутренних дел (полиции).

---

[1] О связи : федеральный закон от 07.07.2003 № 126-ФЗ // СПС «Консультант Плюс».

Разница в процессуальном оформлении между указанными субъектами незначительна – прокурор при возбуждении дела об административном правонарушении выносит постановление, которое должно содержать полный перечень информации, характерной для протокола об административном правонарушении. Соответственно, должностное лицо полиции составляет протокол об административном правонарушении.

КоАП РФ, в отличие от УПК РФ, не содержит дефиниции «прокурор» (в п. 31 статьи 4 УПК РФ под прокурором понимается Генеральный прокурор Российской Федерации и подчиненные ему прокуроры, их заместители и должностные лица органов прокуратуры, участвующие в уголовном судопроизводстве и наделенные соответствующими полномочиями федеральным законом о прокуратуре), поэтому следует ориентироваться на нормы Федерального закона «О прокуратуре Российской Федерации»[1].

Анализ данного акта показал, что легальная дефиниция «прокурор» в нем также отсутствует, а из контекста норм следует, что прокурор – это должностное лицо, которое возглавляет соответствующий орган прокуратуры.

Основываясь на вышеизложенном, считаем, что по аналогии с УПК РФ в текст КоАП РФ следует внести определение категории «прокурор».

С должностными лицами органов внутренних дел (полиции) дело обстоит еще сложнее в силу системной неопределенности данного понятия. Кто же на самом деле перед нами – должностное лицо органа внутренних дел или должностное лицо полиции как составной части органа внутренних дел?

В силу многочисленности различных должностей в органах внутренних дел более подробно лиц, наделенных административно-юрисдикционными полномочиями в органах внутренних дел, на уровне федерального закона определить невозможно, поэтому в настоящее время это определяется Приказом МВД России от 05.05.2012 № 403 «О полномочиях должностных лиц МВД России по составлению протоколов об административных правонарушениях и административному задержанию»[2].

Такое количество должностных лиц разного уровня, в том числе разного уровня образования, крайне затруднительно, если вообще возможно обучить выявлению фактов, образующих объективную сторону состава административного правонарушения, предусмотренного статьей 13.14 КоАП РФ. И в этом, по мнению авторского коллектива, отсутствует необхо-

---

[1] О прокуратуре Российской Федерации : федеральный закон от 17.01.1992 № 2202-1 // СПС «Консультант Плюс».

[2] О полномочиях должностных лиц МВД России по составлению протоколов об административных правонарушениях и административному задержанию : приказ МВД России от 05.05.2012 № 403 (в ред. приказов МВД России от 24.06.2013 № 458, от 19.05.2014 № 426, от 12.01.2015 № 1, от 20.07.2015 № 781, от 12.10.2015 № 969, от 10.02.2016 № 66, от 08.08.2016 № 459, от 07.11.2016 № 698) // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2012. – № 36.

димость. В силу специфичности данного состава достаточно представителей двух подразделений, которые правомочны на составление протоколов – это должностные лица подразделений по исполнению административного законодательства и должностные лица подразделений дознания. Для них возможна разработка программ специальных дисциплин в рамках повышения квалификации, методик выявления правонарушений в данной сфере и методик закрепления доказательственной базы.

Перейдем к рассмотрению положений статьи 13.11 КоАП РФ, которая по охвату охраняемых общественных отношений является частным случаем статьи 13.14. Данная норма изложена в кодексе следующим образом: «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) – влечет предупреждение или наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей; на юридических лиц – от пяти тысяч до десяти тысяч рублей».

Обратим внимание на тот факт, что под действие данной нормы подпадают практически все комплексы действий, осуществляемые органами внутренних дел по отношению к персональным данным.

С точки зрения сущности отношений описанные правонарушения являются неравнозначными по вероятным вредным последствиям их совершения. В частности, нарушение порядка сбора в большинстве случаев влечет за собой накопление персональных данных в объеме и детализации больших, чем те, на которые первоначально имелось разрешение. Если не произошло утечки этой информации, то вредные последствия от такого деяния весьма гипотетичны.

Напротив, когда произошло распространение информации в объеме большем, чем допустимо, вредные последствия наступают сразу. Однако, как видно из статьи, санкции за оба деяния одинаковы и совершенно не могут восприниматься в качестве отражения их потенциальной опасности.

Поэтому авторский коллектив полагает, что необходима дифференциация деяний по степени вредных последствий, наиболее опасным из которых является противоправное распространение. В связи с тем, что нормы статей 13.14 и 13.11 соотносятся между собой как общее и особенное, то есть по отношению к первой вторая является нормой специальной, то целесообразно именно в ее рамках сформулировать состав противоправного распространения (нынешнего разглашения) персональных данных. Отсюда следует, что данную норму целесообразно представить в следующем виде:

«Статья 13.11. Нарушение установленного законом оборота информации о гражданах (персональных данных)

1. Нарушение установленного законом порядка сбора, хранения или использования информации о гражданах (персональных данных) –

влечет ...

2. Противоправное распространение, в том числе разглашение информации о гражданах (персональных данных), –

влечет ...»

Следующей нормой Особенной части КоАП РФ, которую авторский коллектив хотел бы подвергнуть анализу, является ч. 1 статьи 13.28, которая сформулирована следующим образом:

«Нарушение порядка предоставления информации о деятельности государственных органов и органов местного самоуправления, содержащей сведения, относящиеся к информации ограниченного доступа, – влечет наложение административного штрафа на должностных лиц в размере от трех тысяч до пяти тысяч рублей».

Данная статья является относительно новой – она введена Федеральным законом от 31.05.2010 № 108-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[1].

Комментаторы данного правоположения в основном склоняются к тому, что оно направлено на защиту порядка предоставления информации о деятельности государственных органов и органов местного самоуправления, установленного Федеральным законом «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[2].

Действительно, если обратиться к тексту Федерального закона от 14.05.2010 № 108-ФЗ, то можно увидеть его общую направленность на защиту отношений, связанных с расширением уровня освещенности деятельности органов публичной власти. Здесь и изменение норм ст. 5.39 «Отказ в предоставлении информации», и дополнение кодекса ст. 13.27 «Нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети Интернет».

В совокупности в первом приближении получается, что рассматриваемая норма направлена не на защиту отношений по ограничению к доступу к информации конфиденциального характера, а наоборот, на предотвращение излишнего ограничения в доступе к сведениям. Об этом свидетельствует и единственный субъект в составе правонарушения – должностное лицо.

---

[1] О внесении изменений в Кодекс Российской Федерации об административных правонарушениях : федеральный закон от 31.05.2010 № 108-ФЗ // СПС «Консультант Плюс».

[2] См., напр. : комментарий к КоАП РФ / под общ. ред. Н. Г. Салищевой. – М., 2011. – № 330 и др.

Однако более глубокий анализ диспозиции ч. 1 статьи 13.28 показывает, что речь идет о нарушении некоего алгоритма, порядка предоставления такой информации, который должен быть объективирован в виде отдельного акта или части акта. Во всяком случае с точки зрения формальной юридической логики передача сведений ограниченного доступа в принципе возможна в некоторых описанных рамках. Но эти нормативные рамки отсутствуют. И более того, специализированный законодательный акт – Федеральный закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[1] наличие такого алгоритма даже не подразумевает.

Если уж следовать общей логике закона о внесении изменений в КоАП РФ, то на самом деле речь идет о юридической защите права граждан и организаций на доступ к информации о деятельности органов публичной власти. До вступления в силу Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» любой чиновник, не желающий предоставления по запросу какой-либо информации, мог сослаться на то, что доступ к ней ограничен. И гражданин или организация не имели легальной возможности проверки данного факта помимо обращения в прокуратуру или в суд. Но, как показал авторский коллектив в предыдущих разделах настоящего исследования, установление истины в отношении отнесения сведений к категории ограниченного доступа во многих случаях сопряжено с определенными трудностями.

Вышеуказанный закон несколько облегчил решение данной задачи путем наличия в нем следующего правоположения, изложенного в п. 4 статьи 19: «В случае, если запрашиваемая информация относится к категории ограниченного доступа, в ответе на запрос указывается вид, наименование, номер и дата принятия акта, в соответствии с которым доступ к этой информации ограничен. В случае, если часть запрашиваемой информации относится к информации ограниченного доступа, а остальная информация является общедоступной, государственный орган или орган местного самоуправления обязан предоставить запрашиваемую информацию, за исключением информации ограниченного доступа».

Именно необходимость точного указания нормативного акта или отдельной нормы, послужившей основанием для ограничения доступа к испрашиваемой информации, во-первых, существенно ограничивает простор для административного произвола в принятии решения о предоставлении информации, во-вторых, дает данные для проверки обоснованности отказа.

---

[1] Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления : федеральный закон от 09.02.2009 г. № 8-ФЗ // СПС «Консультант Плюс».

Исходя из вышеизложенного, ч. 1 статьи 13.28 КоАП РФ необходимо изложить в следующей редакции:

«*Нарушение установленного порядка оформления отказа в предоставлении сведений о деятельности государственных органов и органов местного самоуправления в случае установления правомерного ограничения в доступе к данным сведениям – ...*».

По мнению авторского коллектива, именно в данной редакции рассмотренная охранительная норма будет иметь наибольший эффект как в плане превенции, так и в плане кары за содеянное.

На этом рассмотрение данной проблемы можно было бы закончить, если бы она не выявила другой, не менее существенной проблемы. Речь идет о том, что в настоящий момент подавляющее большинство нормативных правовых актов, определяющих перечни информации, относимой к сведениям конфиденциального характера, сами ограничены в доступе путем проставления на них ограничительной пометки «Для служебного пользования». Гражданин или организация, получив отказ в предоставлении сведений со ссылкой на закрытый в доступе перечень, опять же самостоятельно правомерность отказа проверить не в состоянии. Получается замкнутый круг.

Но дело не только в этом. Ограничение в доступе к перечням сведений конфиденциального характера, а в большинстве случаев – и к перечням сведений, отнесенных к государственной тайне на ведомственном уровне, резко снижает возможности по оценке обоснованности содержащихся в них положений, в том числе и возможности их научного анализа, что явно не идет на пользу правовому регулированию данных отношений.

По мнению авторского коллектива, необходимо на законодательном уровне предусмотреть запрет на ограничение в доступе к перечням сведений конфиденциального характера, которые действуют в органах публичной власти и организациях. Это позволит существенным образом упорядочить отношения в сфере оборота конфиденциальной информации прежде всего за счет повышения уровня обоснованности введения юридических ограничений на доступ и распространение такой информации.

Последней из норм Особенной части КоАП РФ, которая, по мнению авторского коллектива, должна быть подвергнута анализу в рамках данного раздела исследования, является статья 17.13 «Разглашение сведений о мерах безопасности», которая представлена в кодексе в следующей редакции:

«Разглашение сведений о мерах безопасности, примененных в отношении должностного лица правоохранительного или контролирующего органа либо в отношении его близких, –

влечет наложение административного штрафа на граждан в размере от трехсот до пятисот рублей; на должностных лиц – от пятисот до одной тысячи рублей».

Сам факт нахождения в структуре Особенной части КоАП такой нормы никаких нареканий не вызывает. Однако, если подойти к данной проблеме более системно, то возникает достаточно много вопросов.

Первый из них – проблемы корреляции данной административно-деликтной нормы и соответствующей нормы УК РФ. Там имеется близкая по содержанию статья 320 «Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа» следующего содержания:

«1. Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа, а также его близких, если это деяние совершено в целях воспрепятствования его служебной деятельности, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев либо арестом на срок до четырех месяцев.

2. То же деяние, повлекшее тяжкие последствия, –

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок».

При сравнении положений статьи 17.13 КоАП РФ и ч. 1 статьи 320 УК РФ несложно заметить, что разграничение между административным и уголовным деликтом лежит только в плоскости цели (направленности) деяния – если оно направлено на воспрепятствование служебной деятельности должностного лица, то это уголовно наказуемое деяние. Если такой направленности не установлено, то это административно-правовой деликт.

Как представляется авторскому коллективу, такое разграничение является весьма формальным и совершенно не учитывает потенциальной общественной опасности основного деяния – разглашения определенных сведений, которое может быть осуществлено в том числе и из корыстных побуждений.

Теперь обратим внимание на бросающуюся в глаза разницу в величине санкции – у административно-правовой максимальная ее величина – одна тысяча рублей. У уголовно-правовой, как и положено для таких наказаний, она существенно более весомая.

И если у уголовно-правовой санкции имеется особая направленность, то у административно-деликтной есть собственное основное поле применения – это норма, содержащаяся в статье 16 Федерального закона «О государственной защите судей, должностных лиц правоохранительных

и контролирующих органов»[1], а именно содержащаяся в ней обязанность исполнения решений органов, обеспечивающих безопасность, должностными лицами предприятий, учреждений и организаций, в адрес которых они направлены.

Однако является странным то, что в административно-деликтном плане карается не это неисполнение, а только разглашение, причем столь мягко, что теряется смысл в привлечении к ответственности по данной статье. В результате превентивная роль рассматриваемой нормы КоАП РФ потеряна полностью.

Выход из создавшегося положения, по мнению авторского коллектива, только один – необходимо полностью пересмотреть подход к установлению административной ответственности за вышеуказанные деяния.

Но прежде чем сформулировать конкретные предложения, авторский коллектив хотел бы акцентировать внимание еще на одном существенном моменте: в УК РФ содержится еще одна статья, касающаяся конфиденциальных сведений в сфере обеспечения безопасности физических лиц, – статья 311 «Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса». Данная норма представлена в Особенной части УК РФ в следующей редакции:

1. Разглашение сведений о мерах безопасности, применяемых в отношении судьи, присяжного заседателя или иного лица, участвующего в отправлении правосудия, судебного пристава, судебного исполнителя, потерпевшего, свидетеля, других участников уголовного процесса, а равно в отношении их близких, если это деяние совершено лицом, которому эти сведения были доверены или стали известны в связи с его служебной деятельностью, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до четырехсот восьмидесяти часов, либо ограничением свободы на срок до двух лет, либо арестом на срок до четырех месяцев.

2. То же деяние, повлекшее тяжкие последствия, –

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок».

Конструкция этой охранительной нормы близка к рассмотренной авторским коллективом выше, за исключением ряда незначительных нюансов. Проблема в том, что у этой нормы нет корреспондирующей к ней нормы КоАП РФ. В соответствующем профильном законодательном акте – Федеральном законе «О государственной защите потерпевших, свидетелей

[1] О государственной защите судей, должностных лиц правоохранительных и контролирующих органов : федеральный закон от 20.04.1995 № 45-ФЗ // СПС «Консультант Плюс».

и иных участников уголовного судопроизводства»[1] также имеется норма (статья 22), согласно которой решения органов, обеспечивающих государственную защиту, обязательны для исполнения должностными лицами предприятий, учреждений и организаций.

Помимо указанного, Постановлением Правительства Российской Федерации от 03.03.2007 № 134[2] утверждены Правила защиты сведений об осуществлении государственной защиты потерпевших, свидетелей и иных участников уголовного судопроизводства, соблюдение которых также, по мнению авторского коллектива, должно быть подкреплено охранительной нормой.

Формулировать в КоАП РФ две отдельные статьи, регулирующие рассматриваемые правоотношения, нецелесообразно, так как природа и уровень общественной опасности деяний практически одинаковы. Поэтому диспозицию новой охранительной нормы авторский коллектив предлагает в следующей редакции:

«Статья 17.13. Разглашение сведений о мерах безопасности

1. Несоблюдение либо неполное соблюдение решений органов, обеспечивающих безопасность судей, должностных лиц правоохранительных и контролирующих органов, участников уголовного судопроизводства либо в отношении их близких, –

влечет …

2. Противоправное распространение, в том числе разглашение сведений о мерах безопасности, примененных в отношении лиц, указанных в части первой настоящей статьи, –

влечет …

3. Противоправное распространение, в том числе разглашение сведений о мерах безопасности примененных в отношении лиц, указанных в части первой настоящей статьи, если это деяние создало реальную угрозу их жизни и/или здоровью,–

влечет…».

Установление величины административно-правовой санкции является суверенным правом законодателя. Однако несомненно то, что эта санкция должна иметь величину, которая:

---

[1] О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства : федеральный закон от 20.08.2004 № 119-ФЗ // СПС «Консультант Плюс».

[2] Правила защиты сведений об осуществлении государственной защиты потерпевших, свидетелей и иных участников уголовного судопроизводства : постановление Правительства Российской Федерации от 03.03.2007 № 134 // СПС «Консультант Плюс».

- является реальной оценкой степени общественной опасности (вреда) наказуемого деяния;

- является достаточной карой (мерой ответственности) за содеянное;

- обеспечивает достаточную превенцию от совершения наказуемых деяний в дальнейшем.

Установленные в рассмотренных авторским коллективом в рамках настоящего раздела исследования статьях КоАП РФ санкции ни одному из указанных критериев не отвечают. Для обеспечения их действенности, если законодатель ограничится только административным штрафом, его величину необходимо поднять не менее чем в тридцать и даже в пятьдесят раз, то есть довести до уровня тридцати–пятидесяти тысяч рублей. В противном случае должного эффекта достичь не удастся.

В качестве заключения к данному параграфу исследования авторский коллектив хотел бы отметить следующее.

Проведенный авторским коллективом анализ норм Особенной части КоАП РФ, устанавливающих правонарушения в сфере оборота и защиты конфиденциальной информации, а также санкции за их совершение, показал наличие целого ряда недостатков при их формулировании.

Так, в частности, диспозиция статьи 13.14 сформулирована в общем виде, так что она фактически поглощает правонарушение, предусмотренное статьей 13.11. Диспозиция статьи 13.28 сформулирована с искажением действительного смысла тех отношений, для защиты которых она должна быть предназначена. Статья 17.13 «Разглашение сведений о мерах безопасности», которая должна иметь корреспондирующую связь со статьями 311 и 320 УК РФ, в настоящее время имеет такую связь только с одной из них (статья 320).

ЗАКЛЮЧЕНИЕ

Проведенное исследование, как представляется его авторскому коллективу, достаточно убедительно доказало, что как на законодательном, так и на ведомственном уровне (на примере системы органов внутренних дел) явно прослеживается наличие целого ряда существенных проблем в части системности правового регулирования в сфере оборота и защиты конфиденциальной информации.

Поверхностное, а в ряде случаев пренебрежительно слабое правовое регулирование отношений по обеспечению сохранности сведений конфиденциального характера в федеральных органах исполнительной власти имеет много негативных следствий, среди которых необходимо особо выделить недоверие граждан и организаций к тому, что переданная в органы исполнительной власти информация частного характера будет надежно защищена и использована только в строго определенных законом целях. Это недоверие порождает существенный дисбаланс в информационном взаимодействии между властью и обществом.

Своим исследованием авторский коллектив по естественным причинам не разрешил всех проблем, существующих в данной сфере общественных отношений в связи с их значительностью, разнородностью и разноуровневостью. Однако привлек внимание научной общественности к наличию дисбалансов в этой сфере, их основному абрису, а также представил собственное видение некоторых направлений их разрешения.

Авторский коллектив считает, что в конечном итоге это приведет к существенному улучшению уровня правового регулирования отношений в сфере оборота и защиты конфиденциальной информации в Российской Федерации в целом и в органах внутренних дел в частности.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

I. Нормативные правовые акты

1. В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи (Директива о конфиденциальности и электронных средствах связи) : принята в г. Брюсселе 12.07.2002 // СПС «Консультант Плюс».

2. Конвенция о преступности в сфере компьютерной информации (ETS № 185) : заключена в г. Будапеште 23.11.2001 // СПС «Консультант Плюс».

3. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (ETS № 108) : заключена в Страсбурге 28 января 1981 г. // СПС «Консультант Плюс».

4. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных : федеральный закон от 19.12.2005 № 160-ФЗ // Собрание законодательства РФ. – 26.12.2005. – № 52 (1 ч.). – Ст. 557

5. О защите физических лиц при обработке персональных данных и о свободном обращении таких данных : директива № 95/46/ЕС Европейского парламента и Совета Европейского Союза : принята в г. Люксембурге 24.10.1995 // СПС «Консультант Плюс».

6. Соглашение между Правительством Российской Федерации и Правительством Финляндской Республики о сотрудничестве и борьбе с преступностью : заключено в г. Москве 05.03.1993 // Бюллетень международных договоров. – 1997. – № 4. – С. 20–25.

7. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года : с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ // СПС «Консультант Плюс».

8. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях : федеральный закон от 31.05.2010 № 108-ФЗ // СПС «Консультант Плюс».

9. О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства : федеральный закон от 20.08.2004 № 119-ФЗ // СПС «Консультант Плюс».

10. О государственной защите судей, должностных лиц правоохранительных и контролирующих органов : федеральный закон от 20.04.1995 № 45-ФЗ // СПС «Консультант Плюс».

11. О коммерческой тайне : федеральный закон от 29 июля 2004 г. // СПС «Консультант Плюс».

12. О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд : федеральный закон от 05.04.2013 № 44-ФЗ // СПС «Консультант Плюс».

13. О персональных данных : федеральный закон от 27 июля 2006 г. № 152-ФЗ // СПС «Консультант Плюс».

14. О полиции : федеральный закон от 07 февраля 2011 года № 3-ФЗ (ред. от 12.02.2015 с изм. от 06.04.2015) // СПС «Консультант Плюс».

15. О порядке выезда из Российской Федерации и въезда в Российскую Федерацию : федеральный закон от 15.08.1996 № 114–ФЗ // СПС «Консультант Плюс».

16. О прокуратуре Российской Федерации : федеральный закон от 17.01.1992 № 2202-1 // СПС «Консультант Плюс».

17. О связи : федеральный закон от 07.07.2003 № 126-ФЗ // СПС «Консультант Плюс».

18. Об информации, информатизации и защите информации : федеральный закон от 20.02.1995 № 24-ФЗ // СПС «Консультант Плюс».

19. Об информации, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ // СПС «Консультант Плюс».

20. Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления : федеральный закон от 09.02.2009 г. № 8-ФЗ // СПС «Консультант Плюс».

21. Об объектах культурного наследия (памятниках истории и культуры) народов Российской Федерации : федеральный закон от 25.06.2002 № 73-ФЗ // СПС «Консультант Плюс».

22. Об официальном статистическом учете и системе государственной статистики в Российской Федерации : федеральный закон от 29.11.2007 № 282-ФЗ // СПС «Консультант Плюс».

23. Об электронной подписи : федеральный закон от 06.04.2011 № 63-ФЗ // СПС «Консультант Плюс».

24. О государственной тайне : закон Российской Федерации от 21 июля 1993 г. № 5485-1 // СПС «Консультант Плюс».

25. О частной детективной и охранной деятельности : закон Российской Федерации от 11.03.1992 № 2487–1 // СПС «Консультант Плюс».

26. Перечень сведений конфиденциального характера : указ Президента Российской Федерации от 06 марта 1997 г. № 188 // СПС «Консультант Плюс».

27. О служебной информации ограниченного распространения : постановление совета министров Республики Беларусь от 12.08.2014 № 783 // Национальный правовой интернет-портал Республики Беларусь. 16.08.2017, 5/39265.

28. Об утверждении плана мероприятий по переходу федеральных органов исполнительной власти на безбумажный документооборот при организации внутренней деятельности : распоряжение Правительства РФ от 12.02.2011 № 176-р // СПС «Консультант Плюс».

29. Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации : постановление Правительства Российской Федерации от 12.04.2012 № 287 // СПС «Консультант Плюс».

30. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства РФ от 01 ноября 2012 г. № 1119 // СПС «Консультант Плюс».

31. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти : постановление Правительства Российской Федерации от 03.11.1994 № 1233 // СПС «Консультант Плюс».

32. Правила защиты сведений об осуществлении государственной защиты потерпевших, свидетелей и иных участников уголовного судопроизводства : постановление Правительства Российской Федерации от 03.03.2007 № 134 // СПС «Консультант Плюс».

33. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности : постановление Правительства Российской Федерации от 4 сентября 1995 г. № 870 // СПС «Консультант Плюс».

34. О полномочиях должностных лиц МВД России по составлению протоколов об административных правонарушениях и административному задержанию : приказ МВД России от 05.05.2012 № 403 (в ред. приказов МВД России от 24.06.2013 № 458, от 19.05.2014 № 426, от 12.01.2015 № 1, от 20.07.2015 № 781, от 12.10.2015 № 969, от 10.02.2016 № 66, от 08.08.2016 № 459, от 07.11.2016 № 698) // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2012. – № 36.

35. Об утверждении ведомственной целевой программы «Сельский участковый» : приказ МВД России от 19.11.2013 № 919 // СПС «Консультант Плюс».

36. Об утверждении новой редакции Программы МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел» : приказ МВД России от 20.05.2008 № 435 // СПС «Консультант Плюс».

37. Об утверждении Перечня должностных лиц системы МВД России, пользующихся правом доступа к сведениям, составляющим налоговую тайну : приказ МВД России от 11.01.2012 № 17 (ред. от 12.12.2016) // СПС «Консультант Плюс».

38. Перечень сведений конфиденциального характера органов федерального казначейства Министерства финансов Российской Федерации : приказ Минфина России от 05.01.2004 № 1 // СПС «Консультант Плюс».

39. Перечень сведений ограниченного доступа, не содержащих сведений, составляющих государственную тайну, (конфиденциального характера) Министерства финансов Российской Федерации : приказ Минфина России от 17.06.2014 № 162 // СПС «Консультант Плюс».

40. Перечень сведений конфиденциального характера : постановление главы администрации Волгоградской области от 24.01.2006 № 54 // СПС «Консультант Плюс».

41. Перечень сведений конфиденциального характера : постановление Главы администрации Мариинского муниципального района от 07.05.2013 № 438–П // СПС «КонсультантПлюс».

42. Перечень сведений конфиденциального характера : распоряжение главы администрации Омской области от 08.01.1998 № 9-р // СПС «Консультант Плюс».

43. Перечень сведений конфиденциального характера муниципального дошкольного образовательного учреждения «Шелемишевский детский сад» Скопинского муниципального района Рязанской области : приказ директора от 29.07.2013 № 15 // URL: www.shelemishevsad.ucod.ru.

44. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. СТО БР ИББС-1.0-2014» : распоряжение Банка России от 17.05.2014 № Р-399 // Вестник Банка России. – 2014. – № 48–49.

II. Диссертации, авторефераты диссертаций

45. Бурдов С. Н. Административно-правовые режимы конфиденциальной информации : дис. ... канд. юрид. наук : 12.00.14 / Бурдов Сергей Николаевич. – СПб., 2015. – 196 с.

46. Иванов Д. В. Конфиденциальная информация как условие трудового договора : дис. ... канд. юрид. наук : 12.00.05 / Иванов Дмитрий Викторович. – М., 2009. – 156 с.

47. Караваев А. А. Административно-правовое регулирование оборота и защиты конфиденциальной информации в органах внутренних дел : дис. … канд. юрид. наук : 12.00.14 / Караваев Александр Александрович. – Краснодар, 2015. – 220 с.

48. Кротов А.В. Конституционное право граждан на информацию и свободу информации : дис. ... канд. юрид. наук : 12.00.02 / Кротов Андрей Владиславович. – Казань, 2007. – 210 с.

49. Павлов И. Ю. Правовое обеспечение доступа к официальной информации : дис. ... канд. юрид. наук : 12.00.14 / Павлов Иван Юрьевич. – М., 2008. – 187 с.

50. Семашко А. В. Правовые основы оборота информации с ограниченным доступом (конфиденциальной информации) в Российской

Федерации : автореф. ... дис. канд. юрид. наук : 12.00.14 / Семашко Александр Викторович. – М., 2008. – 168 с.

51. Соколова О. С. Административно-правовые режимы конфиденциальной информации : дис. ... канд. юрид. наук : 12.00.14 / Соколова Ольга Сергеевна – СПб., 2005. – 159 с.

52. Строгонова И. В. Правовой режим конфиденциальной информации (гражданско-правовой аспект) : автореф. … дис. канд. юрид. наук : 12.00.03 / Строгонова Ирина Викторовна – Екатеринбург, 2004. – 178 с.

53. Федотова О. А. Административная ответственность за правонарушения в сфере обеспечения информационной безопасности : дис. … канд. юрид. наук : 12.00.14 / Федотова Ольга Анатольевна. – Москва, 2003. – 195 с.

54. Швецов А. В. Защита информации в сфере служебной тайны в деятельности ОВД : правовой аспект : дис. … канд. юрид. наук : 05.13.19 / Швецов Андрей Владимирович. – М., 2005. – 217 с.

III. Литература. Монографии

55. Загородников С. Н. Чужие тайны и их защита: нормативно-правовые аспекты / С. Н. Загородников, Д. А. Максимов // Российский следователь. – 2014. – № 3. – С. 44.

56. Камалова Г. Г. Исторические особенности правовой охраны служебной информации ограниченного доступа (служебной тайны) в советский период / Г. Г. Камалова // Вестник Удмуртского университета. – 2014. – Вып. 2. – С. 144.

57. Комментарий к Уголовному кодексу Российской Федерации / отв. ред. В. М. Лебедев. – М., 2013. – С. 630.

58. Комментарий к Уголовному кодексу Российской Федерации : в 2 т. / под ред. А. В. Бриллиантова. – М., 2015. – С. 434.

59. Конституция Российской Федерации. Доктринальный комментарий / под рук. Ю. А. Дмитриева, Ю. И. Скуратова. – М. : Статут, 2013. – С. 180.

60. Павлов И. Ю. Современные проблемы правового регулирования государственной и служебной тайны в России / И. Ю. Павлов // Ленинградский юридический журнал. – 2013. – С. 35.

61. Саранчук Ю. М. Квалификация административных правонарушений, предусмотренных статьей 13.11 КоАП РФ / Ю. М. Саранчук // Административное право и процесс. – 2014. – № 10. – С. 60.

62. Сингх С. Книга шифров. Тайна история шифров и их расшифровки / С. Сингх. – М., 2007. – С. 9.

63. Система защиты информации VipNet : курс лекций / под общ. ред. О. А. Чефрановой. – М., 2014. – С. 171.

64. Соболева Т. А. История шифровального дела в России / Т. А. Соболева. – М. : ОХМА-ПРЕСС, 2002.

65. Толковый словарь русского языка / сост. С. И. Ожегов. – М., 1956. – С. 591.

66. Топорков А. А. Криминалистика : учебник / А. А. Топорков. – М., 2012.

67. Трофимов С. В. Правовое обеспечение инновационного развития промышленного производства / С. В. Трофимов. – Иркутск., 2010. – С. 4.

68. Фатьянов А. А. Правовое обеспечение безопасности информации в Российской Федерации / А. А. Фатьянов. – М., 2001. – С. 161.

IV. Статьи

69. Антопольский А. А. Законодательство о служебной тайне как средство борьбы с коррупцией: перспективы развития / А. А. Антопольский // Информационные ресурсы России. – 2010. – № 6. – С 17–28.

70. Атаманов Г. А. О законодательстве Российской Федерации в области защиты различного вида тайн и необходимости его корректировки / Г. А. Атаманов // Право и безопасность. – 2011. – № 3-4. – С. 21–29.

71. Афанасьева О. В. Доступ к информации как институт национального государства / О. В. Афанасьева // Полис : Политические исследования. – 2010. – № 5. – С. 146–149.

72. Загородников С. Н. Чужие тайны и их защита: нормативно-правовые аспекты / С. Н. Загородников, Д. А. Максимов // Российский следователь. – 2014. – № 3. – С. 44.

73. Камалова Г. Г. Исторические особенности правовой охраны служебной информации ограниченного доступа (служебной тайны) в советский период / Г. Г. Камалова // Вестник Удмуртского университета. – 2014. – Вып. 2. – С. 144.

74. Павлов И. Ю. Современные проблемы правового регулирования государственной и служебной тайны в России / И. Ю. Павлов // Ленинградский юридический журнал. – 2013. – С. 35.

75. Саранчук Ю. М. Квалификация административных правонарушений, предусмотренных статьей 13.11 КоАП РФ / Ю. М. Саранчук //Административное право и процесс. – 2014. – № 10. – С. 60.

76. Соколова Г. А. Охрана коммерческой и служебной тайны в рамках трудовых отношений / Г. А. Соколова // Делопроизводство и документооборот на предприятии. – 2011. – № 5. – С. 56–60.

77. Терещенко Л. К. Специальные правовые режимы информации / Л.К. Терещенко // Журнал зарубежного законодательства и сравнительного правоведения. – 2011. – № 2 (27). – С. 69–75.

78. Фатьянов А. А. Концептуальные основы обеспечения безопасности на современном этапе / А. А. Фатьянов // Безопасность информационных технологий. – 1999. – № 1. – С. 26–40.

Приложение

Результаты анкетирования сотрудников правоохранительных органов по вопросам административно-правового регулирования оборота и защиты конфиденциальной информации в органах внутренних дел[1]

№	Вопрос	Варианты ответов	Распределение ответов
1.	Имеете ли Вы представление о существовании правового института конфиденциальной информации?	а) имею б) частично в) не имею г) иное	36,80% 50% 12,5% 0,70%
2.	Знакомы ли Вы с действующим законодательством, регулирующим общественные отношения в сфере оборота конфиденциальной информации?	а) да б) нет в) частично	17,37% 26,38% 56,25%
3.	Пользуетесь ли Вы сведениями конфиденциального характера при осуществлении должностных полномочий?	а) да б) нет в) в случае необходимости привлекаю специалиста	59,03% 25% 15,97%
4.	Следует ли законодательно закрепить термин «конфиденциальная информация»?	а) да б) нет в) затрудняюсь ответить	63,88% 6,25% 29,87%
5.	Допустимо ли раскрытие сведений конфиденциального характера коллегам по работе (например, в неформальной беседе и т.д.)?	а) да б) нет в) затрудняюсь ответить	6,25% 87,5% 6,25%
6.	Как Вы оцените работу ОВД по защите информации конфиденциального характера?	а) неудовлетворительно б) удовлетворительно в) хорошо г) отлично	12,5% 54,86% 26,38% 6,26%
7.	Известно ли Вам о существовании технологий удаленного доступа к информационным ресурсам (сбор, копирование, блокирование, изменение, уничтожение и т.д. информации на расстоянии)?	а) известно б) неизвестно в) иное	46,53% 47,22% 6,25%
8.	Существует ли, на Ваш взгляд, необходимость разработки внутреннего регламента по работе с конфиденциальной информацией вне зависимости от формы ее представления?	а) да б) нет в) иное	72,22% 24,30% 3,48%
9.	Существует ли, на Ваш взгляд, необходимость законодательного закрепления «Перечня сведений конфиденциального характера»?	а) да б) нет в) иное	82,64% 15,28% 2,08%
10.	По Вашему мнению, существует ли потребность в совершенствовании административной ответственности за правонарушения в сфере конфиденциальной информации?	а) да б) нет в) иное	83,33% 14,58% 2,09%

[1] В приложении не приводятся иные результаты, которые были получены при анкетировании сотрудников правоохранительных органов, в частности, данные об их возрасте, образовательном уровне, месте жительства, профессиональном стаже, занимаемой должности и т.д.

Научное издание

Занина Татьяна Митрофановна
Караваев Александр Александрович

АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ОБОРОТА И ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Монография

Редактор Н. Ф. Палихова
Корректор А. С. Власова
Компьютерная верстка В. В. Павлов

Подписано в печать 29.01.2018. Формат 60×84 1/16
Усл. печ. л. 6,04
Тираж 60 экз. Заказ № 11

Воронежский институт МВД России
394051 Воронеж, просп. Патриотов, 53

Типография Воронежского института МВД России
394051 Воронеж, просп. Патриотов, 53