Научная статья
УДК 34.07 + 004.056.5
DOI: 10.37973/KUI.2022.51.52.006

# К ВОПРОСУ О ПРАВОВОМ СТАТУСЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Адель Миннурович Каримов,
Казанский юридический институт МВД России, Казань, Россия,
karimov485@mail.ru

***Аннотация***

**Введение:** в статье на основе анализа современного российского законодательства, ведомственных подзаконных нормативных актов, регламентирующих основания и порядок доступа и распространения компьютерной информации, юридической литературы рассмотрены проблемы правовой регламентации защиты ведомственной информации ограниченного доступа и ограниченного распространения.

**Материалы и методы:** методологическую основу исследования составила совокупность общенаучных и частнонаучных методов познания: диалектический, догматический, семантический, формально-логический, методы анализа и синтеза. Материалами исследования послужили нормы федерального законодательства Российской Федерации, подзаконных нормативных актов, научная литература.

**Результаты исследования:** внесены предложения по преодолению коллизии в праве в результате применения нормативного акта большей юридической силы, а также восполнению правового пробела в результате принятия Федерального закона «О служебной тайне и режиме её правовой защиты».

**Обсуждение и заключения:** выявлен ряд проблем, возникающих в правовой регламентации порядка обращения с информацией ограниченного распространения в органах внутренних дел. Обоснована необходимость принятия Федерального закона «О служебной тайне и режиме её правовой защиты».

*Ключевые слова: тайна; ведомство; защита; информация, доступ*



**Для цитирования:** Каримов А.М. К вопросу о правовом статусе информации ограниченного распространения в органах внутренних дел Российской Федерации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 3 (49). С. 61 – 68. DOI: 10.37973/KUI.2022.51.52.006

Scientific article
UDC 34.07 + 004.056.5
DOI: 10.37973/KUI.2022.51.52.006

# THE LEGAL STATUS OF INFORMATION OF LIMITED DISTRIBUTION IN INTERNAL AFFAIRS BODIES OF THE RUSSIAN FEDERATION

Adel Minnurovich Karimov,
Kazan Law Institute of MIA of Russia, Kazan, Russia,
karimov485@mail.ru

***Abstract***

**Introduction:** the article based on the analysis of modern Russian legislation, departmental bylaws regulating the grounds and procedure for access and dissemination of computer information, legal literature, examined the problems of legal regulation of the protection of departmental information of limited access and limited distribution. The legal collision and correlated legal gap in the issue of legal regulation of the order of treatment of information of limited distribution in the bodies of internal affairs were revealed.

**Materials and Methods:** the methodological basis of the study was a set of general scientific and private scientific methods of knowledge: dialectical, dogmatic, semantic, formal-logical, methods of analysis and synthesis. Materials of research were the norms of federal legislation of the Russian Federation, subordinate legislation, scientific literature.

**Results:** proposals for overcoming conflicts in the law by applying a normative act of greater legal force, as well as filling the legal gap as a result of the publication of the Federal Law "On Official Secrets" were made.

**Discussion and Conclusions:** a number of problems arising in the legal regulation of the procedure for handling information of limited distribution in the internal affairs bodies has been identified. The necessity of publishing the Federal law "On official secrecy" is substantiated.

*Keywords: secret; agency; protection; information, access*



**For citation:** Karimov A.M. The Legal Status of Information of Limited Distribution in Internal Affairs Bodies of the Russian Federation // Bulletin of the Kazan Law Institute of MIA of Russia. 2022. T. 13. No 3 (49). P. 61 – 68. DOI: 10.37973/KUI.2022.51.52.006

## Введение

Органы внутренних дел в своей оперативно-служебной деятельности, как и другие институты государственной исполнительной власти, активно используют достижения современной науки и техники. С использованием современных информационно-теллекоммуникационнных технологий по защищенным каналам связи передаются масштабные пакеты данных между подразделениями ОВД и иными правоохранительными органами, органами государственной и муниципальной власти, общественными объединениями и организациями. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» декларирует по этому поводу следующее: «полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру»[1]. В науке же в связи с этим констатируется: информационный ресурс является доминантным фактором развития не только производственной сферы, но и экономической системы в целом, информационная насыщенность выступает объективным критерием достигнутой зрелости традиционных факторов производства [1]; коммуникационные технологии оказывают существенное влияние на все сферы общества [2].

Развитие информационно-коммуникационных технологий обусловливает и рост цифровой преступности и иных инцидентов в сфере информационных технологий. Так, по данным официальной статистики МВД России за январь-сентябрь 2021 г., на территории Российской Федерации было зарегистрировано 510 396 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, из них более половины (267 613) преступлений являются тяжкими или особо тяжкими[2].

Специалисты Лаборатории «Касперского» приводят следующие данные о состоянии инцидентов в сфере информационной безопасности за 10 месяцев 2021 года:

2.024 млрд вредоносных онлайн-атак заблокировано;

77.4 млн уникальных вредоносных артефактов детектировано: скрипты, эксплоиты, исполняемые файлы;

614 млн уникальных вредоносных URL-адресов найдено и заблокировано;

96.2% всех атак исходят от 10 стран (топ 3: Германия (30.86%), США (26.53%), Доминиканская Республика (21.58%);

91.841 пользователей защищены от шифровальщиков.

## Обзор литературы

Правовую базу исследования составили Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ; Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции»; Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» и др.

Выявить особенности норм о порядке обращения с конфиденциальной информацией в РФ, определить специфику этой информации, классифицировать сведения в деятельности ОВД, подлежащие защите в ОВД, позволили работы О.М. Хохловой [1], Т.В. Зверевой [2], В.Ф. Васюкова [3], А.В. Булыжкина, О.Э. Николаева [4], В.А. Кемпфа [5].

[1] О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ. СПС «КонсультантПлюс» (дата обращения: 15.11.2021).

[2] Состояние преступности: Главный информационно-аналитический центр МВД России. URL: https://x№--b1aew.x№--p1ai/dejatel№ost/statistics (дата обращения: 15.11.2021).

**Материалы и методы**

Методологическую основу статьи составили диалектический подход к познанию юридической природы информации ограниченного распространения в РФ, содержания ее видов, общенаучные и частные методы исследования (анализ, синтез, дедукция, индукция, статистический метод), которые применялись при изучении различных правовых явлений, их сравнении и формулировании предложений по совершенствованию российского законодательства.

Материалами исследования послужили положения действующего российского уголовного законодательства, научная юридическая литература.

**Результаты исследования**

ОВД имеют возможность использовать информационно-телекоммуникационную сеть "Интернет", автоматизированные информационные системы, интегрированные банки данных. Компьютерная информация, собираемая, используемая и хранящаяся в информационных системах ОВД, может стать предметом киберугроз. Для того чтобы эффективно противостоять этим угрозам, смоделировать возможные инциденты в сфере информационных технологий и на основе этих моделей выстроить стойкую эшелонную систему мер защиты компьютерной информации, необходимо в первую очередь определиться с тем, какую именно служебную информацию, исходя из действующего законодательства, нам необходимо защищать, каковы структура и форма представления этой информации, в чем ее особенность и каков потенциальный ущерб интересам ОВД в информационной сфере в случае несанкционированного распространения такой информации.

Согласно примечанию к ст. 272 Уголовного кодекса Российской Федерации от 13.06.1996 № 63-ФЗ: «под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи»[1].

Компьютерной информации свойственны определенные черты, которые определяют характерные особенности деятельности с электронными носителями информации:

– существенный объем при малых габаритах носителя, сжимаемости и последующем извлечении;

– скорость обработки, легкое разрушение, возможность преобразования в понятный вид;

– возможность передачи по каналам связи, доступность для нескольких пользователей одновременно;

– возможность поиска исключительно на электронных носителях в машиночитаемой форме;

– формирование, трансформация, копирование и применение компьютерной информации реализовывается с помощью микропроцессорных устройств, которые могут читать (записывать) соответствующие носители;

– метаданные, в т.ч. дата и время создания файла, внесенные в него изменения, используемое программное обеспечение, в некоторых ситуациях – используемое оборудование и т.п.;

– способность к копированию, т.е. перенос с одного электронного носителя на другой, в котором копия полностью (идентична) оригиналу, включая сами сведения и метаданные [3].

Объектами информационной безопасности ОВД являются данные, информация, информационные ресурсы и инфраструктура ОВД. Иными словами, информация, которая подвержена угрозам, – это информационные ресурсы, содержащие сведения и данные, использующиеся сотрудниками ОВД в процессе своей профессиональной и служебной деятельности.

К наиболее важным объектам обеспечения информационной безопасности в правоохранительной сфере, иначе говоря, к ведомственным объектам критической инфраструктуры относятся:

информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Для проведения всестороннего исследования необходимо обозначить виды сведений, которые становятся объектом информационных процессов[2] в ОВД. Эти информационные процессы обусловлены необходимостью решения оперативно-служебных задач, стоящих перед ведомством. Содержание данной информации предполагает необходимость ее защиты право-

[1] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ. СПС «КонсультантПлюс» (дата обращения: 15.11.2021).

[2] Под информационными процессами понимаются получение, хранение, обработка и передача информации.

выми, организационными, техническими, программными и криптографическими методами.

1. Согласно ст. 17 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» «полиция имеет право обрабатывать данные о гражданах, необходимые для выполнения возложенных на нее обязанностей, с последующим внесением полученной информации в банки данных о гражданах»[1].

Простой анализ характера баз данных ведомственных информационных систем, в том числе и служебных сервисов ИСОД МВД России, указывает на то, что большинство из них являются фактографическими ИСПДн (информационными системами персональных данных). Таким образом, можно констатировать, что наиболее масштабным видом информации ограниченного доступа и ограниченного распространения, которая может быть подвержена угрозам информационной безопасности в ОВД, выступают персональные данные[2]. К персональным данным следует относить следующие сведения:

- идентификационные сведения;
- биографические сведения;
- сведения личного характера;
- информацию, включающую семейное положение;
- информацию, включающую социальное положение;
- информацию о здоровье и др.

2. Следующим немаловажным видом информации, которая может быть подвержена киберугрозам, являются сведения, относящиеся к государственной тайне. Согласно Закону РФ от 21.07.1993 № 5485-1 «О государственной тайне» под государственной тайной понимаются: «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации»[3].

Характерными для ОВД как субъекта ОРД сведениями, составляющими государственную тайну, является информация, получаемая при осуществлении оперативно-розыскной деятельности. Одной из главных проблем в процессе обеспечения результативности ОРД в настоящее время, по нашему внутреннему убеждению, является повышение уровня безопасности информационного обеспечения данной деятельности, поскольку при реализации коммуникативных мероприятий, которые составляют целостность информационного обеспечения, существуют многочисленные риски, из-за которых цели ОРД могут быть не достигнуты.

По мнению О.Э. Николаева, в целом ОРД можно представить как информационную деятельность, которая включает в себя совокупность процессов обработки информации, важнейшим из которых является поиск информации, необходимой для решения задач ОРД [4].

Электронная форма представления информации дает возможность результативно обрабатывать имеющиеся данные посредством программного обеспечения, особенно когда они представлены в структурированной форме, которая представлена различными информационными системами. В связи с цифровой формой представления таких сведений становится актуальным вопрос защиты этих данных от угроз информационной безопасности.

3. Сведения, составляющие тайну следствия и судопроизводства[4], а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» и другими нормативными правовыми актами Российской Федерации, также являются информацией, подверженной угрозам информационной безопасности ОВД.

4. Наряду со сведениями, относящимся к государственной тайне, следует отметить и сведения, которые не являются секретными, но при этом ограничены в распространении. Некоторые авторы называют такие сведения «служебной тайной» ОВД, которая связана с функционированием самой системы МВД России [5].

Проведенный нами анализ российского законодательства дает основание утверждать, что

[1] О полиции: Федеральный закон от 07.02.2011 № 3-ФЗ. СПС «КонсультантПлюс» (дата обращения: 15.11.2021).

[2] О некоторых мерах, направленных на обеспечение выполнения МВД России обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»: приказ МВД России от 21.12.2017 № 949. СПС «КонсультантПлюс» (дата обращения: 16.03.2022); Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах органов внутренних дел Российской Федерации: приказ МВД России от 06.07.2012 № 678 . СПС «КонсультантПлюс» (дата обращения: 15.02.2022).

[3] О государственной тайне: Закон РФ от 21.07.1993 № 5485-1. СПС «КонсультантПлюс» (дата обращения: 16.03.2022).

[4] Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 18.12.2001 № 174-ФЗ. СПС «КонсультантПлюс» (дата обращения: 15.02.2022); Гражданский процессуальный кодекс Российской Федерации: Федеральный закон от 14.11.2002 № 138-ФЗ. СПС «КонсультантПлюс» (дата обращения: 04.04.2022); Арбитражный процессуальный кодекс Российской Федерации: Федеральный закон от 24.07.2002 № 95-ФЗ. СПС «КонсультантПлюс» (дата обращения: 15.02.2022).

нормотворец часто использует словосочетание «служебная тайна» в тексте различных по характеру, социальной направленности и юридической силе правовых актах и документах. Так, к примеру, в пункте 3 указа Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» к таковым отнесены служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (*служебная тайна*)»[1]. Однако еще раз подчеркнем, что Федерального закона «О служебной тайне и режиме её правовой защиты» нет. В законе закреплена иная правовая категория – служебная информация ограниченного распространения. К таким сведениям законодатель относит несекретную информацию, касающуюся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами[2].

Согласно приказу МВД России от 09.11.2018 № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России» «к служебной информации ограниченного распространения в системе МВД России относятся несекретная информация, касающаяся деятельности органов, организаций, подразделений системы МВД России, ограничения, на распространение которых диктуются служебной необходимостью»[3]. При этом необходимо обратить внимание на некоторые законодательные противоречия. Положения данного подзаконного акта, по сути, закрепляют правовую защиту и ограничения в доступе к определенному роду информации, которую в науке иногда называют «служебной тайной». Между тем ст. 5 Федерального закона № 149 «Об информации, информационных технологиях и защите информации»[4] четко устанавливает, что доступ к информации может быть ограничен только федеральными законами. Налицо правовая коллизия. Постановление Правительства Российской Федерации и ведомственный подзаконный акт ограничивают доступ к информации, что противоречит положениям правового акта, имеющего большую юридическую силу, который указывает, что такие ограничения могут быть регламентированы только федеральным законом. Так, доступ к персональным данным граждан ограничен положениями Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ[5], к тайне следствия и судопроизводства – УПК РФ, ГПК РФ и КАС РФ, к государственной тайне – Законом РФ от 21.07.1993 № 5485-1 «О государственной тайне». Даже коммерческая тайна и соответствующий правовой режим не остались без внимания законодателя. Названные вопросы регулируются Федеральным законом «О коммерческой тайне» от 29.07.2004 № 98-ФЗ[6] и четвертой частью ГК РФ. А вот юридический статус «родственной» правовой категории – «служебной тайны» – и тематического правового режима ее защиты на данный момент нормотворцем не определен. Сказанное позволяет резюмировать факт наличия не только правовой коллизии между положениями постановления Правительства Российской Федерации от 3 ноября 1994 г. № 1233, приказа МВД России № 755 и ст. 5 Федерального закона № 149, но и вытекающего из нее правового пробела, который необходимо восполнить. Эта потребность обусловлена тем, что информация, признаваемая постановлением Правительства Российской Федерации № 1233 и приказом МВД России № 755 сведениями ограниченного доступа и распространения, не может быть оставлена без комплексной, эшелонной правовой защиты.

Представляется верным признать в качестве документа третьего эшелона правовых средств защиты служебной информации приказ МВД России № 755 в его действующей редакции. Этот акт детально регламентирует порядок обращения с информацией ограниченного распространения в ОВД РФ и с точки зрения законодательной техники может выступать в качестве документа, конкретизирующего положения актов второго и первого «рубежей» защиты. Второй рубеж – это нормы постановления Правительства Российской Федерации от 3 ноября 1994

[1] Об утверждении Перечня сведений конфиденциального характера: указ Президента Российской Федерации от 06.03.1997 № 188 (ред. от 13.07.2015) // Собрание законодательства Российской Федерации.1997. № 10. Ст. 1127.

[2] Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности: постановление Правительства Российской Федерации от 03.11.1994 № 1233.

[3] О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России: приказ МВД России от 09.11.2018 № 755. СПС «КонсультантПлюс» (дата обращения: 15.03.2022).

[4] Собрание законодательства Российской Федерации. 2006. № 31 (1 ч.). Ст. 3448.

[5] Собрание законодательства Российской Федерации. 2006. № 31 (1 ч.). Ст. 3451.

[6] Собрание законодательства Российской Федерации. 2004. № 32. Ст. 3283.

г. № 1233. В качестве первого, «статутного» документа должен выступать правовой акт большей юридической силы. Исходя из требований ст. 5 Федерального закона № 149, подобным актом может стать только Федеральный закон, а именно авторская редакция проекта Федерального закона «О служебной тайне и режиме ее правовой защиты», который будет устанавливать наиболее общие положения, связанные с правовой регламентацией сведений ограниченного распространения.

Отметим, что еще в 2011 году был снят с рассмотрения Государственной Думы Федерального Собрания проект Федерального закона № 124871-4 «О служебной тайне», внесенный депутатами Государственной Думы Федерального Собрания Российской Федерации В.В. Бобыревым, А.Н. Волковым, М.И. Гришанковым, В.В. Дятленко, В.И. Илюхиным, Н.С. Леоновым, В.В. Маргеловым, А.М. Розуваном еще в 2004 году. Обратим внимание, что «базовый» НПА в сфере информации – ФЗ № 149 – был принят только в 2006 году.

В пояснительной записке к проекту ФЗ «О служебной тайне и режиме её правовой защиты» было указано следующее: необходимость системного правового регулирования института служебной тайны вызвана рядом причин, в том числе отсутствием в законодательстве единого подхода к соответствующей категории информации ограниченного доступа; многочисленными примерами незаконного распространения (продажи) информации, аккумулируемой в органах государственной власти и относящейся либо к личности, либо к деятельности хозяйствующих субъектов; ограничениями на распространение информации, накладываемыми по своему усмотрению руководителями органов государственной власти и государственными (муниципальными) служащими на представление информации гражданам, общественным организациям, средствам массовой информации[1].

**Обсуждение и заключения**

В целях преодоления существующей правовой коллизии и восполнения пробела представляется необходимым законодательное закрепление в праве института служебной тайны в Российской Федерации и режима правовой защиты таких сведений. Предлагается двухконтурная модель правовой регламентации общественных отношений, связанных с доступом и порядком распространения сведений, с пометкой «для служебного пользования». В качестве третьего «рубежа» защиты нами рассматривается действующая редакция приказа МВД России от 09.11.2018 № 755 «О некоторых вопросах обращения со служебной информацией ограниченного распространения в системе МВД России». Второй – постановление Правительства Российской Федерации от 3 ноября 1994 г. № 1233. Эти документы будут конкретизировать положения общего акта большей юридической силы, т.е. «тематического» федерального закона. Исходя из предписаний действующего законодательства, на таком уровне эти правоотношения не могут регламентироваться подзаконными актами и могут быть урегулированы только федеральным законом. Это базовая правовая оболочка (первый эшелон юридической защиты) общественных отношений, связанных с порядком допуска и обращения со служебными сведениями ограниченного распространения. В связи со сказанным нами сформулировано предложение по совершенствованию действующего российского законодательства в результате разработки, публичного обсуждения и принятия Федерального закона «О служебной тайне и режиме ее правовой защиты». Такое решение позволит восполнить правовой пробел и одновременно преодолеть юридическую коллизию, обозначенную выше.

В качестве основных положений предлагается закрепить следующее:

**статья 1. Сфера действия Федерального закона «О служебной тайне и режиме ее правовой защиты»**

Федеральный закон «О служебной тайне и режиме ее правовой защиты» направлен на урегулирование общественных отношений, возникающих в процессе допуска граждан и должностных лиц к сведениям, составляющим служебную тайну, их распространения, отнесения сведений к служебной тайне, снятия ограничений на доступ к ним в целях защиты прав, свобод и законных интересов граждан, организаций, публичных образований.

**Статья 2. Субъекты Федерального закона «О служебной тайне и режиме ее правовой защиты»**

Нормы Федерального закона «О служебной тайне и режиме её правовой защиты» обязательны для исполнения гражданами, юридическими лицами, должностными лицами федеральных органов государственной власти, органов власти субъектов РФ, органов местного самоуправле-

[1] Проект Федерального закона № 124871-4 «О служебной тайне» (ред., внесенная в Государственную Думу Федерального Собрания Российской Федерации, текст по состоянию на 24.12.2004). Документ опубликован не был. СПС «КонсультантПлюс» (дата обращения 12.01.2022).

ния, которые осуществляют поиск, обработку, хранение, передачу и распространение сведений, составляющих служебную тайну на основании Федерального закона, иных федеральных законов и принимаемых в соответствии с ними нормативных правовых актов, а также лицами, получившими доступ к сведениям, составляющим служебную тайну в соответствии с настоящим Федеральным законом, у которых такая обязанность возникает в силу должностных или трудовых обязанностей.

**Статья 3. Основные понятия, используемые в Федеральном законе «О служебной тайне и режиме ее правовой защиты»**

Для целей Федерального закона используются следующие основные понятия:

**Служебная тайна (сведения, составляющие служебную тайну)** – несекретные сведения конфиденциального характера, которые образуются в результате документационного обеспечения управления юридических лиц, федеральных органов государственной власти, органов власти субъектов РФ, органов местного самоуправления, публичное и бесконтрольное распространение которых может нанести ущерб их интересам в информационной сфере либо иным образом отрицательно отразиться на реализации функций и задач, стоящих перед названными публичными образованиями и организациями;

**Носители сведений, составляющих служебную тайну** – материальные объекты, в том числе физические поля, в которых соответствующие сведения находят свое отображение в виде символов, образов, сигналов;

**Отнесение сведений к служебной тайне** – регламентированный Федеральным законом «О служебной тайне и режиме её правовой защиты» процесс наложения ограничений на доступ к сведениям, составляющим служебную тайну, и на их распространение;

**Режим служебной тайны** – правовой режим ограничений и запретов на доступ и распространение сведений, составляющих служебную тайну.

## СПИСОК ИСТОЧНИКОВ

1. Хохлова О.М., Рожкова А.К., Хохлова А.В. Информационная безопасность в системе национальной безопасности современного российского общества // Инновационное развитие науки: фундаментальные и прикладные проблемы. Петрозаводск: Международный центр научного партнерства «Новая Наука», 2021. С. 73 – 90.
2. Зверева Т.В. Возможности налогового администрирования по минимизации налоговых рисков в цифровой экономике // Инновационное развитие экономики. 2017. № 5 (41). С. 86 – 90.
3. Васюков В.Ф., Булыжкин А.В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Рос. следователь. 2016. № 6. С. 3 – 8.
4. Николаев О.Э. Угрозы информационной безопасности при осуществлении оперативно-розыскной деятельности и основные пути их отражения // Труды Академии управления МВД России. 2020. № 3 (55). С. 30 – 37.
5. Кемпф В.А. Обеспечение информационной безопасности в органах внутренних дел: учебное пособие. Барнаул: БЮИ МВД России, 2019. 63 с.

## REFERENCES

1. Hohlova O.M., Rozhkova A.K., Hohlova A.V. Informacionnaya bezopasnost' v sisteme nacional'noj bezopasnosti sovremennogo rossijskogo obshchestva // Innovacionnoe razvitie nauki: fundamental'nye i prikladnye problemy. Petrozavodsk: Mezhdunarodnyj centr nauchnogo partnerstva «Novaya Nauka», 2021. S. 73 – 90.
2. Zvereva T.V. Vozmozhnosti nalogovogo administrirovaniya po minimizacii nalogovyh riskov v cifrovoj ekonomike // Innovacionnoe razvitie ekonomiki. 2017. № 5 (41). S. 86 – 90.
3. Vasyukov V.F., Bulyzhkin A.V. Iz"yatie elektronnyh nositelej informacii pri rassledovanii prestuplenij: nereshennye problemy pravovogo regulirovaniya i pravoprimeneniya // Ros. sledovatel'. 2016. № 6. S. 3 – 8.
4. Nikolaev O.E. Ugrozy informacionnoj bezopasnosti pri osushchestvlenii operativno-rozysknoj deyatel'nosti i osnovnye puti ih otrazheniya // Trudy Akademii upravleniya MVD Rossii. 2020. № 3 (55). S. 30 – 37.
5. Kempf V.A. Obespechenie informacionnoj bezopasnosti v organah vnutrennih del: uchebnoe posobie. Barnaul: BYuI MVD Rossii, 2019. 63 s.

**Информация об авторе:**
**Каримов Адель Миннурович,** кандидат юридических наук, старший преподаватель кафедры экономики, финансового права и информационных технологий в деятельности органов внутренних дел Казанского юридического института МВД России, karimov485@mail.ru

Автор прочитал и одобрил окончательный вариант рукописи.

**Information about the author:**
**Karimov Adel' M.,** Candidate in Law (Research doctorate), Senior Lecturer of the Department of Economics, Financial Law and Information Technologies in the Activity of Internal Affairs Bodies, the Kazan Law Institute of MIA of Russia, karimov485@mail.ru

The author has read and approved the final version of the manuscript.

Статья получена: 08.04.2022.
Статья принята к публикации: 16.09.2022.
Статья опубликована онлайн: 29.09.2022.

Против размещения полнотекстовой версии статьи в открытом доступе в сети Интернет не возражаю.