МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Тюменский институт повышения квалификации сотрудников МВД России

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ОПЕРАТИВНО-РАЗЫСКНОЙ ИНФОРМАЦИИ

Терминологический словарь

Тюмень
2019

УДК 343.102
ББК 67.99(2)91
О-64

Рекомендовано к изданию редакционно-издательским советом
Тюменского института повышения квалификации сотрудников МВД России

Рецензенты:
заместитель начальника кафедры информационного и технического обеспечения органов внутренних дел Дальневосточного юридического института МВД России кандидат технических наук *В.С. Дунин*;
доцент кафедры оперативно-разыскной деятельности
Омской академии МВД России кандидат юридических наук *Л.А. Бакланов*

Составители:
Анисина С.С., канд. филос. наук, доцент; *Достов В.В.*;
Усманов Р.А., канд. юрид. наук

О-64 **Организация** деятельности подразделений оперативно-разыскной информации: терминологический словарь / предисл. Р.А. Усманов. Тюмень: Тюменский институт повышения квалификации сотрудников МВД России, 2019. 56 с.

ISBN 978-5-93160-290-5

Терминологический словарь посвящен основным направлениям информационно-аналитического обеспечения деятельности органов внутренних дел. В базовых терминах и определениях раскрываются вопросы организации информационно-аналитического обеспечения оперативно-розыскной деятельности органов внутренних дел; формирования, ведения и использования информационной системы оперативно-розыскной информации; использования информационных ресурсов МВД России и иных государственных органов и организаций.

Издание адресовано сотрудникам подразделений оперативно-разыскной информации системы МВД России, преподавателям, слушателям образовательных организаций системы МВД России.

УДК 343.102
ББК 67.99(2)91

ISBN 978-5-93160-290-5

Предисловие

Становление и развитие информационных технологий привело к тому, что в настоящее время невозможно представить ни одну сферу человеческой деятельности, в которой не использовались бы технические и программные средства, позволяющие автоматизировать процессы собирания, обработки и выдачи информации. В деятельность практически всех учреждений и организаций внедрена современная компьютерная техника, на основе которой созданы автоматизированные рабочие места. Компьютеризированные рабочие места соединены в локальные и региональные компьютерные сети с подключением к международной компьютерной сети Интернет. От использования автоматизированных информационно-поисковых систем произошел переход к разработке и внедрению интегрированных банков данных.

Изменения сказались и на деятельности органов внутренних дел. Понимание необходимости обеспечения оперативных подразделений органов внутренних дел актуальной и достаточной информацией привело к созданию в соответствии с приказом МВД России от 7 августа 2001 г. № 725 Управления оперативно-разыскной информации Службы криминальной милиции МВД России. Подразделения оперативно-разыскной информации занимаются оперативно-аналитическим и информационным сопровождением оперативно-розыскной деятельности органов внутренних дел, осуществляют информационное сопровождение процесса выявления и раскрытия преступлений.

Специфические задачи, стоящие перед сотрудниками подразделений оперативно-разыскной информации, разнородность сведений, необходимых для раскрытия и расследования преступлений, обусловливают необходимость оперирования знаниями из различных научных областей (теория оперативно-розыскной деятельности, информатика, уголовное право, уголовный процесс, криминалистика, судебная экспертиза, документоведение). В каждой из перечисленных наук используется свой категориальный аппарат, и у сотрудников подразделений оперативно-разыскной информации может вызывать затруднение толкование того или иного термина.

В связи с этим перед составителями данного терминологического словаря стояла цель исследовать основные направления деятельности подразделений оперативно-разыскной информации, ознакомиться с соответствующей терминологией, выбрать наиболее значимые термины и привести их дефиниции, закрепленные в нормативных правовых актах либо содержащиеся в научной литературе.

В словаре приведены термины, используемые в информатике, оперативно-розыскной деятельности, криминалистике и судебной экспертизе.

Список сокращений

АИПС – автоматизированная информационно-поисковая система
АС – автоматизированная система
АСНИ – автоматизированная система научных исследований
АСУ – автоматизированная система управления
АСУП – автоматизированная система управления предприятиями
АСУТП – автоматизированная система управления технологическими процессами
БД – база данных
ЕАСС – единая автоматизированная система связи
ИНС – искусственная нейронная сеть
ИС ОРИ – информационная система оперативно-розыскной информации
МВД России – Министерство внутренних дел Российской Федерации
НСД – несанкционированный доступ
ОВД – органы внутренних дел
ОРМ – оперативно-розыскное мероприятие
ОРД – оперативно-розыскная деятельность
САПР – система автоматизированного проектирования
СМЭВ – система межведомственного электронного взаимодействия
СНГ – Содружество Независимых Государств
СОИ – система обработки информации
СУБД – система управления базами данных
УК РФ – Уголовный кодекс Российской Федерации
ФЗ об ОРД – Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»
ЭВМ – электронно-вычислительная машина
ЭЦП – электронная цифровая подпись

Термины и определения

HTML (англ. Hyper Text Markup Language – язык гипертекстовой разметки) – язык гипертекстовой разметки документов в международной компьютерной сети Интернет. *Большинство веб-страниц содержит описание разметки на языке HTML (или XHTML). Язык HTML интерпретируется браузерами; полученный в результате интерпретации форматированный текст отображается на экране монитора компьютера или мобильного устройства.*

Identi-kit – идентификационный комплект для изготовления составных (синтетических) портретов путем наложения друг на друга прозрачных пленок с изображением элементов внешности. *Предложен в 1965 г. В отечественной практике был разработан и использовался аналог identi-kit – идентификационный комплект рисунков (ИКР).*

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций. *В зависимости от вида деятельности выделяют следующие виды АС: автоматизированные системы управления (АСУ), системы автоматизированного проектирования (САПР), автоматизированные системы научных исследований (АСНИ) и др. В зависимости от вида управляемого объекта (процесса) различают автоматизированные системы управления технологическими процессами (АСУТП), автоматизированные системы управления предприятиями (АСУП) и др.*

Автоматизированная система идентификации отпечатка пальца – в биометрии: специализированная биометрическая система, которая сравнивает заданное изображение пальца с эталонами изображений пальца, записанными в базе данных.

Автоматизированное индексирование – индексирование, технология которого предусматривает использование формальных процедур, осуществляемых с помощью вычислительной техники, и включает применение интеллектуальных процедур при принятии основных решений о составе поискового образа.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

Автоматизированный документальный поиск – документальный поиск с использованием ЭВМ.

Администратор защиты – субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Администрирование базы данных – управление базой данных (БД) как единым информационным ресурсом организации с целью эффективного обслуживания коллектива пользователей. *Администрирование БД предполагает выполнение комплекса мероприятий, обеспечивающих точность, непротиворечивость, полноту, защиту и доступность данных в нужной форме, в нужном месте и в нужное время. Это касается вопросов обеспечения информацией как пользователей, так и приложений, работающих с БД. В рамках администрирования БД обеспечивается безопасность БД, осуществляется восстановление БД, производится ее обслуживание, осуществляется обучение пользователей, обеспечивается резервное копирование данных, организуется сопровождение БД, производится тестирование системы, организуется управление доступом пользователей к данным, обеспечивается целостность данных. Ответственность за поддержание ресурсов БД может быть поделена между администратором данных и администратором базы данных.*

Адресно-справочная база данных – отсылочная база данных, в которой указаны адреса хранения искомых данных.

Аккредитация – официальное признание органом по аккредитации компетентности физического или юридического лица в части выполнения работы в определенной области оценки соответствия.

Акт – документ, удостоверяющий информацию, полученную в процессе осуществления оперативно-розыскных мероприятий. Оформляется оперативным работником с участием посторонних лиц (понятых, специалистов, должностных лиц и т.д.) или лицами, привлеченными для проведения оперативно-розыскных мероприятий.

Анализ изображений – в биометрии: процесс выделения из изображения неизобразительной информации, а также описания (интерпретации) и представления изображения с помощью его компонентов, свойств и зависимостей.

Анализ информационного риска – систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации.

Аналитико-синтетическая переработка – преобразование документов в процессе их анализа и извлечения необходимой информации, а также оценка, сопоставление, обобщение и представление информации в виде, соответствующем запросу.

Аналитическая работа – вид оперативно-розыскной деятельности органов внутренних дел, направленный на решение наиболее важных, актуальных и сложных оперативно-розыскных задач, связанных с установлением сущности, причин и тенденций как отдельных фактов, событий, явлений, так и в целом преступной деятельности и борьбы с ней. *Основное содержание аналитической работы составляют оценка информации и ее исследование. В аналитической работе выделяют следующие важнейшие функции: объяснительную, прогностическую и эвристическую.*

Аналитическая разведка – получение необходимой информации посредством анализа данных, имеющихся в находящихся в свободном доступе источниках или же добытых негласными способами. *Аналитическую разведку необходимо рассматривать как составную часть разведки в целом – как элемент разведывательного цикла.*

Анатомические признаки внешности – пол, возраст, рост, телосложение, антропологические черты внешности, строение тела, головы, лица и его элементов. *Особое внимание уделяется лицу человека как наиболее индивидуализирующему личность при ее зрительном восприятии. Кожные покровы лица (головы), в особенности те из них, которые характеризуются близкорасположенной костно-хрящевой основой черепа, относительно устойчивы в течение всей жизни человека (лоб, нос, уши и др.).*

Архив – учреждение или структурное подразделение организации, осуществляющее хранение, комплектование, учет и использование архивных документов.

Архивный документ – материальный носитель с зафиксированной на нем информацией, который имеет реквизиты, позволяющие его идентифицировать, и подлежит хранению в силу значимости указанных носителя и информации для граждан, общества и государства.

Архивный фонд Российской Федерации – исторически сложившаяся и постоянно пополняющаяся совокупность архивных документов, отражающих материальную и духовную жизнь общества, имеющих историческое, научное, социальное, экономическое, политическое и культурное значение, являющихся неотъемлемой частью историко-культурного наследия народов Российской Федерации, относящихся к информационным ресурсам и подлежащих постоянному хранению.

Ассоциативный доступ к данным – способ доступа к данным, позволяющий обращаться к ячейкам запоминающего устройства в соответствии с признаками хранимых в них данных.

Аттестация объектов информатизации – комплекс организационно-технических мероприятий, в результате которых посредством специального документа – аттестата соответствия подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических

документов по безопасности информации, утвержденных Гостехкомиссией России.

Аудиторская проверка информационной безопасности в организации – периодический независимый и документированный процесс получения свидетельств аудита и объективной оценки с целью определить степень выполнения в организации установленных требований по обеспечению информационной безопасности.

База данных (БД) – совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимая от прикладных программ.

Банк данных – автоматизированная информационно-поисковая система, состоящая из одной или нескольких баз данных и системы хранения, обработки и поиска информации в них.

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Безопасность информационная – состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования и т.п.

Биометрика – область знаний, представляющая методы измерения физических характеристик (или персональных поведенческих черт) человека и методы их сравнения с аналогичными данными в базе данных для целей идентификации или аутентификации человека.

Биометрическая идентификация – способ идентификации личности по отдельным специфическим биометрическим признакам (идентификаторам), присущим конкретному человеку. *Данные признаки можно условно разделить на две основные группы: а) генетические и физиологические параметры (геометрия ладони, отпечаток пальца, рисунок радужной оболочки или сетчатки глаза, геометрические характеристики лица, структура ДНК (сигнатура); б) индивидуальные поведенческие особенности, присущие каждому человеку (почерк, речь и пр.).*

Биометрическая система – автоматизированная система, способная реализовывать функции: фиксации биометрической выборки от конечного пользователя; извлечения биометрических данных из этой выборки; сравнения биометрических данных с одним или большим количеством эталонов; принятия решения о том, насколько они соответствуют; индикации о том, была ли достигнута идентификация или проверка идентичности.

Биометрическая характеристика – измеримая физическая характеристика человека, используемая в процессе его проверки на подлинность или идентичность санкционированному пользователю.

Биометрические технологии – отрасль (науки и производства), представляющая методы и технические средства получения и использования биометрических данных человека в целях его идентификации (верификации, аутентификации или распознавания). *В Б.т. используются как физические биометрические характеристики человека – отпечатки пальцев, геометрия руки, изображения радужной оболочки и сетчатки глаза, голос, видео- и термоизображения лица, подпись (а в последнее время изображения ушей, отпечатки губ и запах человека), так и поведенческие биометрические характеристики, например, манера работы на клавиатуре компьютера, динамика написания рукописного текста, стиль и манера походки.*

Биометрия – система распознавания людей по одной или более физическим или поведенческим чертам. *В области информационных технологий биометрические данные используются в качестве формы управления идентификаторами доступа и контроля доступа. Кроме того, биометрический анализ используется для выявления людей, которые находятся под наблюдением*.

Блок накопления данных – совокупность технических средств, содержащая накопители данных, средства управления накопителями, средства приема, коммутации, распределения и передачи сигналов, обеспечивающая запись и воспроизведение больших массивов данных с произвольным доступом к данным.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Ввод данных – операция чтения данных с носителя, запись этих данных в память данных.

Ведение базы данных – деятельность по обновлению, восстановлению и перестройке структуры базы данных с целью обеспечения ее целостности, сохранности и эффективности использования.

Ведомственная первичная сеть – совокупность физических цепей, типовых и внутрипроизводственных каналов передачи и сетевых трактов, образованная на базе сетевых узлов, сетевых станций, оконечных устройств и линий передачи ведомств. *Типовые физические цепи, типовые каналы передачи и сетевые тракты ведомственной первичной сети входят в первичную сеть единой автоматизированной системы связи.*

Ведомственные сети связи – сети электросвязи министерств и иных федеральных органов исполнительной власти, создаваемые для удовлетво-

рения производственных и иных специальных нужд, имеющие выход на сети связи общего пользования.

Вербальный информационно-поисковый язык – информационно-поисковый язык, в котором для представления своих лексических единиц используются слова и выражения естественного языка в их орфографической форме.

Верификация – дополнительная проверка результата распознавания с целью установления истинности этого результата. Реализуется аналогично аутентификации.

Взаимоувязанная сеть связи – комплекс технологически сопряженных сетей связи общего пользования и ведомственных сетей электросвязи на территории Российской Федерации, обеспеченный общим централизованным управлением, независимо от ведомственной принадлежности и форм собственности.

Взвешивание поисковых терминов – определение меры значимости поискового термина с целью ограничить выдачу либо рассортировать ее в соответствии со степенью релевантности.

Владелец закрытого ключа электронной цифровой подписи – физическое или юридическое лицо, которое создает ключи электронной цифровой подписи с использованием принадлежащих ему на законном основании средств электронной цифровой подписи.

Владелец сертификата ключа подписи – физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы).

Владелец сертификата ключа проверки электронной подписи – лицо, которому в порядке, установленном Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи», выдан сертификат ключа проверки электронной подписи.

Владелец электронной цифровой подписи – учреждения Банка России, вычислительный центр, кредитная организация (филиал) или другой клиент Банка России, электронная цифровая подпись которого зарегистрирована в порядке, установленном договором между Банком России и его клиентом.

Вневедомственные учеты – учеты, созданные вне МВД России для информационного обслуживания государственных, общественных, частных структур и граждан.

Внемашинная информационная база автоматизированной системы – часть информационной базы АС, представляющая собой совокуп-

ность документов, предназначенных для непосредственного восприятия человеком без применения средств вычислительной техники.

Внешний облик человека – наружный вид человека, обусловленный совокупностью информации о нем, воспринимаемой зрительно. *Элементы В.о.ч. и их признаки делятся на собственные и сопутствующие. Собственные – это элементы и их признаки, которые характеризуют строение тела человека (головы; туловища: плечи, грудь, спина, таз; верхних и нижних конечностей) и различные проявления его жизнедеятельности, которые свойственны (присущи) человеку и неотъемлемо ему принадлежат. Они делятся на морфологические (общефизические, анатомические) и функциональные. Сопутствующие – это элементы и их признаки, которые не являются неотъемлемыми для В.о.ч., но естественно дополняют его и в определенной мере позволяют характеризовать собственные элементы и их признаки. К ним относятся постоянные элементы (одежда, обувь, головные уборы) и носимые (зонт, очки, слуховой аппарат, украшения).*

Внешняя схема базы данных – схема базы данных, поддерживаемая системой управления базы данных для приложений.

Внутренняя схема базы данных – схема базы данных, определяющая представление данных в среде хранения и пути доступа к ним.

Внутригосударственный обмен документами – обмен документами между библиотеками, информационными центрами и другими организациями внутри одной страны.

Время регистрации (в биометрии) – время, которое должна затратить биометрическая система на получение биометрического образа (эталона) пользователя, включая фиксацию биометрической выборки от пользователя системы и извлечение биометрических данных (образа) из этой выборки.

Входная информация автоматизированной системы – информация, поступающая в АС в виде документов, сообщений, данных, сигналов, необходимая для выполнения функций АС.

Вывод данных – операция чтения данных в памяти данных и последующая их запись на носитель данных или отображение на экране.

Габитоскопия – отрасль криминалистической техники, изучающая теоретические положения и технико-криминалистические средства и методы сбора, изучения и использования данных о внешнем облике человека.

Гипертекстовая база данных – текстовая база данных, записи в которой содержат связи с другими записями, позволяющими компоновать ансамбли записей на основе их логической связанности.

Главная справочная картотека – систематическая библиографическая картотека, отражающая документы в соответствии с информацион-

ными потребностями основных групп читателей и абонентов данной библиотеки или информационного центра.

Государственная стандартизация – национальная стандартизация, проводимая на уровне одной страны – участницы Соглашения о проведении согласованной политики в области стандартизации, метрологии, сертификации и аккредитации в этих областях деятельности.

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Государственный архив – федеральное государственное учреждение, создаваемое Российской Федерацией, или государственное учреждение субъекта Российской Федерации, создаваемое субъектом Российской Федерации, которые осуществляют комплектование, учет, хранение и использование документов Архивного фонда Российской Федерации, а также других архивных документов.

Государственный оборонный заказ – правовой акт, предусматривающий поставки продукции для федеральных государственных нужд в целях поддержания необходимого уровня обороноспособности и безопасности Российской Федерации: боевого оружия, боеприпасов, военной техники, другого военного имущества, комплектующих изделий и материалов, выполнение работ и предоставление услуг, а также экспортно-импортные поставки в области военно-технического сотрудничества Российской Федерации с иностранными государствами в соответствии с международными договорами Российской Федерации.

Государственный стандарт – национальный стандарт страны, национальный орган по стандартизации которой входит в Евразийский совет по стандартизации, метрологии и сертификации.

Грамматика информационно-поискового языка – правила формирования поисковых образов и поисковых предписаний из лексических единиц информационно-поискового языка.

Гриф ограничения доступа к документу – реквизит официального документа, свидетельствующий об особом характере информации, ограничивающий круг пользователей документа.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Гриф согласования – реквизит официального документа, выражающий согласие учреждения или его органа, не являющегося автором документа, с его содержанием.

Группа распространения – имя, идентифицирующее группу клиентов, которым будет доставлена данная статья в дополнение к клиентам группы новостей.

Групповая адресация – адресация, при которой по одному адресу осуществляется обращение к группе абонентов.

Дактилоскопическая криминалистическая регистрация – сбор, сосредоточение, обработка и использование идентификационных сведений о задержанных, арестованных и осужденных к лишению свободы с использованием отпечатков их рук на специальных бланках – дактилоскопических картах. *Д.к.р. используется для отождествления личности, розыска без вести пропавших, получения информации о состоявшемся ранее дактилоскопировании.*

Дактилоскопия – раздел криминалистической техники, изучающий папиллярные узоры и их следы в целях идентификации человека и криминалистического учета.

Данные – информация, обработанная и представленная в формализованном виде для дальнейшей обработки.

Декларирование соответствия – форма подтверждения соответствия продукции требованиям технических регламентов.

Дело – совокупность документов или отдельный документ, относящиеся к одному вопросу или участку деятельности федерального органа исполнительной власти.

Делопроизводство – деятельность, обеспечивающая создание официальных документов и организацию работы с ними в федеральных органах исполнительной власти.

Дескрипторный информационно-поисковый язык – информационно-поисковый язык, предназначенный для координатного индексирования документов и информационных запросов посредством дескрипторов и (или) ключевых слов.

Дескрипторный словарь – словарь дескрипторного информационно-поискового языка, в котором приведены в общем алфавитном ряду дескрипторы и их синонимы без указания других отношений лексических единиц. *Дескрипторный словарь является упрощенным вариантом информационно-поискового тезауруса, в котором зафиксированы преимущественно или только синонимические связи.*

Диалоговая информационно-поисковая система – автоматизированная информационно-поисковая система, обеспечивающая осуществление диалогового поиска.

Диалоговый поиск – автоматизированный информационный поиск, при котором пользователь автоматизированной системы может формули-

ровать информационные запросы в диалоговом режиме, корректировать их в процессе поиска и получать промежуточные результаты.

Диспетчер доступа – технические, программные и микропрограммные элементы комплекса средств защиты, реализующие концепцию диспетчера доступа.

Документ – материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения.

Документ секретный – текстовой, графический или иной материал, содержащий закрепленные различными способами секретные сведения и оформленный в установленном порядке.

Документальная база данных – база данных, в которой каждая запись отражает конкретный документ, содержит его библиографическое описание и, возможно, иную информацию о нем.

Документальная информационно-поисковая система – информационно-поисковая система, предназначенная для поиска документов и (или) сведений о них.

Документальный информационно-поисковый язык – информационно-поисковый язык, предназначенный для индексирования документов (частей документов) с целью последующего хранения и поиска.

Документальный поиск – информационный поиск, при котором объектами поиска являются документы.

Документация на автоматизированную систему – комплект взаимоувязанных документов, полностью определяющих технические требования к АС, проектные и организационные решения по созданию и функционированию АС.

Допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений.

Достоверность данных – свойство данных не иметь скрытых ошибок.

Доступ к сведениям, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Естественный язык – язык, словарь и грамматические правила которого обусловлены практикой применения и не всегда формально зафиксированы.

Жестикуляция – комплекс движений рук, плеч (иногда головы) человека, которыми он сопровождает свою речь, чтобы придать ей большую выразительность. *При описании жестикуляции фиксируют ее темп (быстрая, медленная), выразительность (оживленная, энергичная, вялая), характер жестов и их содержание (указательная, изобразительная и т.п.).*

Заверенная копия документа – копия документа, на которой в соответствии с установленным порядком проставляют необходимые реквизиты, придающие ей юридическую силу.

Закрытый ключ электронной цифровой подписи – уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи.

Закрытый тип данных – тип данных с открытой спецификацией, но закрытой реализацией.

Запретная дата документа – дата, означающая, что документы, возникшие ранее ее, экспертизе их научной и практической ценности не подвергаются и уничтожению не подлежат.

Защита информации – защита сведений, отнесенных в установленном порядке к государственной или служебной тайне, от иностранных технических разведок и от ее утечки по техническим каналам. *З.и. осуществляется путем выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Правительством Российской Федерации.*

Защита информации от непреднамеренного воздействия – защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного воздействия – защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводя-

щих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Защита информации от несанкционированного доступа – защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

Защита информации от преднамеренного воздействия – защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях.

Защита информации от разглашения – защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Защита информации от утечки – защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации (иностранными) разведками и другими заинтересованными субъектами.

Защищаемая информационная система – информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями, содержащимися в нормативных правовых документах, или устанавливаемыми собственником информации. *Собственниками информации могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.*

Защищенное средство вычислительной техники, защищенная автоматизированная система – средство вычислительной техники (автоматизированная система), в котором реализован комплекс средств защиты.

Знак соответствия национальным стандартам – защищенный и зарегистрированный в установленном в Российской Федерации порядке знак, выданный и применяемый в соответствии с ГОСТ Р 1.9, информирующий, что обеспечивается необходимая уверенность в том, что идентифицированная должным образом продукция соответствует всем положениям

(требованиям) конкретного национального стандарта (национальных стандартов) на данную продукцию.

Значимость данных – свойство данных сохранять ценность для потребителя с течением времени (составляющая временных свойств).

Идентификатор доступа – уникальный признак субъекта или объекта доступа.

Идентификационная информация – комплекс выделенных в процессе изучения объекта сведений о его свойствах, отражающих принадлежность объекта к определенному множеству – роду (группе) объектов, и о неоднородности свойств одного (идентифицируемого) объекта, отраженных в другом (идентифицирующем).

Идентификационный комплект рисунков (ИКР) – набор штриховых рисунков элементов лица. Предназначался для изготовления по показаниям очевидцев композиционно-рисованных портретов (субъективных портретов). *Состоял из 1238 рисунков элементов лиц мужчин и 727 элементов лиц женщин. Рисунки помещались в альбомы-реестры и дублировались на ацетатных прозрачных пленках. Пленки размещались в специальном контейнере по видам элементов лица. Портрет составлялся путем наложения пленок друг на друга на экране монтажно-демонстрационного устройства (входящего в комплект), совмещая их в любом порядке и легко заменяя. Для репродукции составленного портрета в комплекте имелся фотоаппарат.*

Идентификация – отождествление, установление совпадения чего-либо с чем-либо; опознание лица или вещи на основании неизменяемых признаков. Является составной частью исследования предметов и документов как ОРМ.

Идентификация биометрическая – процедура, базирующаяся на технологии распознавания образов и предназначенная для однозначного определения личности человека на основе его биометрических характеристик при сравнении их с заданными эталонами.

Идентифицируемый объект – объект, отождествление которого составляет задачу процесса идентификации.

Идентифицирующий объект – объект, с помощью которого решается задача идентификации. *Среди И.о. выделяются образцы для сравнительного исследования.*

Идентичность данных – свойство данных соответствовать состоянию объекта; нарушение идентичности связано со старением данных по рассогласованию признаков (составляющих временных свойств).

Иерархическая база данных – база данных, реализованная в соответствии с иерархической моделью данных.

Изготовитель базы данных – лицо, организовавшее создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов.

Изображение человека объективное – изображение лица, фигуры человека в объективных портретах (фотопортрет, кино- и видеокадр, рентгенограмма, голограмма), слепках, масках и т.п.

Изображение человека субъективное – изображение лица, фигуры человека, изготовленное на основе и в соответствии с представлением о внешности определенного лица, – субъективные портреты (рисованные, различные композиционные портреты, словесный портрет).

Имитовставка – отрезок информации фиксированной длины, полученной по определенному правилу из открытых данных и ключа и добавленный к зашифрованным данным для обеспечения имитозащиты.

Имитозащита – защита системы шифрованной связи от навязывания ложных данных.

Индекс дела, номер дела – цифровое и (или) буквенно-цифровое обозначение дела в номенклатуре дел организации, наносимое на его обложку.

Индекс доступа – совокупность данных, обеспечивающих соответствие между значениями ключей порций данных и адресами этих порций или областей пространства памяти, в которых они находятся, с целью повышения скорости доступа к порции данных.

Индексно-последовательный набор данных – набор данных, каждая из физических записей которого снабжена своим ключом порции данных так, что обеспечивается прямой доступ к ним с использованием индексов доступа и поиска по ключу, а также последовательный доступ в соответствии с их упорядоченностью по значениям ключей.

Инициирование – создание условий для запуска процесса обработки данных.

Интегрированная автоматизированная система – совокупность двух или более взаимоувязанных АС, в которой функционирование одной из них зависит от результатов функционирования другой (других) так, что эту совокупность можно рассматривать как единую АС.

Интерактивный режим – режим взаимодействия процесса обработки информации системы обработки информации с человеком, выражающийся в разного рода воздействиях на этот процесс, предусмотренных механизмом управления конкретной системы и вызывающих ответную реакцию процесса.

Интересы государства в информационной сфере – создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражда-

нина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности Российской Федерации, политической, экономической и социальной стабильности, безусловное обеспечение законности и правопорядка, развитие равноправного и взаимовыгодного международного сотрудничества.

Интерпол – международная организация уголовной полиции, созданная группой стран с целью взаимодействия правоохранительных органов различных государств в борьбе с межгосударственными (транснациональными) преступлениями (международным терроризмом, наркобизнесом и т.д.), а также оказания помощи в розыске преступников и похищенного.

Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационная безопасность Российской Федерации – состояние защищенности в информационной сфере ее национальных интересов, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Информационная система – организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информационная система общего пользования – информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

Информационная система оперативно-розыскной информации (ИС ОРИ) – информационная система, содержащая структурированную оперативно-розыскную информацию, в том числе и из открытых источников, используемую для обеспечения проведения оперативно-розыскных мероприятий, конечной целью которых является раскрытие и профилактика преступлений.

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационная услуга – предоставление информации определенного вида потребителю по его запросу.

Информационное обеспечение – совокупность информационных ресурсов и услуг, предоставляемых для решения управленческих и научно-технических задач в соответствии с этапами их выполнения.

Информационное обслуживание – обеспечение пользователей необходимой информацией, осуществляемое информационными органами и службами путем предоставления информационных услуг.

Информационно-поисковая система – совокупность справочно-информационного фонда и технических средств информационного поиска в нем.

Информационно-поисковый тезаурус – нормативный словарь дескрипторного информационно-поискового языка с зафиксированными в нем парадигматическими отношениями лексических единиц. *Парадигматические отношения указывают общность или противопоставление значений и использования лексических единиц.*

Информационно-справочная служба – телематическая служба, предназначенная для предоставления пользователям услуг хранения информации и обработки запросов пользователей об адресах физических и юридических лиц.

Информационные системы класса 1 (К1) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных.

Информационные системы класса 2 (К2) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных.

Информационные системы класса 3 (К3) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных.

Информационные системы класса 4 (К4) – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Информационные системы персональных данных – совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Информационный запрос – текст, выражающий информационную потребность.

Информационный массив – банк данных, сайт, геоинформационная система и др.

Информационный менеджмент – организованное управление работой предприятия, фирмы или объединения, осуществляемое на основе комплексного использования всех видов информации, имеющихся как на самом предприятии, в фирме или объединении, так и за его пределами.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их регистрации и представления.

Информация конфиденциальная – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Исключение документов, рекомплектование – отбор, изъятие из фонда и снятие с учета непрофильных, устаревших, излишне дублетных, ветхих документов, а также снятие с учета утраченных документов.

Искусственная нейронная сеть (ИНС) – математическая модель, а также ее программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма. *ИНС представляет собой систему соединенных и взаимодействующих между собой простых процессоров (искусственных нейронов). Такие процессоры обычно довольно просты (особенно в сравнении с процессорами, используемыми в персональных компьютерах). Каждый процессор подобной сети имеет дело только с сигналами, которые он периодически получает, и сигналами, которые он периодически посылает другим процессорам. Тем не менее, будучи соединенными в достаточно большую сеть с управляемым взаимодействием, такие по отдельности простые процессоры вместе способны выполнять довольно сложные задачи.*

Истинность данных – свойство данных не иметь искажений, намеренно внесенных человеком (составляющая свойства достоверности).

История болезни – основной первичный медицинский документ, составляемый на больного (испытуемого), находящегося на амбулаторном, стационарном обследовании или лечении в медицинском учреждении. *Содержит демографические данные, данные субъективного и объективного анамнеза, обследований и наблюдений за состоянием больного (испытуемого) в течение всего времени нахождения его в медицинском учреждении, результаты проведенных исследований и лечебно-профилактических мероприятий, оценку индивидуальных особенностей состояния здоровья больного (испытуемого) и течения его заболевания, сведения об исходе заболевания при выписке или переводе больного (испытуемого). В случае смерти больного в историю болезни вносятся данные вскрытия и гистологических исследований. Хранится в архиве медицинского учреждения. Используется при проведении судебно-медицинских и судебно-психиатрических экспертиз, для опознания трупов и др.*

Источник угрозы безопасности информации – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Канал электросвязи единой автоматизированной системы связи – путь прохождения сигналов электросвязи, образованный последовательно соединенными каналами и линиями вторичной сети единой автоматизированной системы связи (ЕАСС) при помощи станций и узлов вторичной сети ЕАСС, обеспечивающий при подключении оконечных устройств вторичной сети передачу сообщения от его источника к получателю (получателям).

Картотека – система несброшюрованных карточек, содержащих тематическую информацию, расположенных в алфавитном порядке для облегчения поиска.

Квалифицированный сертификат ключа проверки электронной подписи – сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее – уполномоченный федеральный орган).

Класс защищенности средств вычислительной техники, автоматизированной системы – определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации.

Классификационная структура – совокупность отношений классов в классификационной системе. *Классификационная структура включает отношения классов всех уровней – иерархии.*

Классификационная таблица – материальное представление классификационной системы.

Классификационная цепь – совокупность последовательных классов классификационной системы, в которой каждый класс, кроме первого, подчинен предыдущему классу.

Классификационное дерево – совокупность классификационных цепей, имеющих общий подчиняющий класс.

Классификационный индекс – поисковый образ, построенный средствами классификационного информационно-поискового языка.

Классификационный информационно-поисковый язык – информационно-поисковый язык, предназначенный для индексирования документов (частей документов) и информационных запросов посредством понятий и кодов какой-либо классификационной системы.

Классификационный признак – элемент содержания понятия, который позволяет отнести данное понятие к определенному классу в некоторой классификационной системе.

Классификационный ряд – совокупность классов классификационной системы, которые непосредственно подчинены одному классу.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Коллективный доступ (в интерфейсной системе) – одновременный доступ нескольких абонентов интерфейса к общим ресурсам системы обработки информации.

Комбинация оперативная – искусственное создание условий, вынуждающих проверяемых лиц действовать в интересах оперативного работника.

Комплекс средств защиты – совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

Комплектование архива – систематическое пополнение архива документами в соответствии с его профилем и действующим законодательством.

Комплектование фонда – совокупность процессов выявления, отбора, заказа, приобретения, получения и регистрации документов, соответствующих задачам библиотеки, информационного центра.

Конвертирование данных – изменение формы представления данных в соответствии с определенными правилами при сохранении содержащейся в них информации.

Конечный пользователь – потребитель информации, который использует данные, полученные от информационно-поисковой системы, для целей, не связанных с эксплуатацией самой системы.

Контроль (надзор) за соблюдением требований технических регламентов – проверка выполнения юридическим лицом или индивидуальным предпринимателем требований технических регламентов к продукции или к связанным с ними процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации и принятие мер по результатам проверки.

Контроль данных – технологическая операция, состоящая в сравнении значений показателей, характеризующих состояние данных с определенными значениями.

Контроль технического состояния – проверка соответствия значений параметров объекта требованиям технической документации и определение на этой основе одного из заданных видов технического состояния в данный момент времени.

Конфигурация системы обработки информации – совокупность функциональных частей системы обработки информации и связей между ними, обусловленная основными техническими характеристиками этих функциональных частей, а также требованиями решаемых задач.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Концептуальная схема базы данных – схема базы данных, определяющая представление базы данных, единое для всех ее приложений и не зависящее от используемого в системе управления этой базой данных представления данных в среде хранения и путей доступа к ним.

Кооперированная каталогизация – совместная деятельность нескольких библиотек или информационных центров на основе разделения функций при подготовке библиографической информации.

Координированное комплектование – согласованное комплектование двух и более библиотек, информационных центров с целью разграничения в приобретении документов по тематике, видам, устранения неоправданного дублирования и расширения репертуара приобретаемых документов. *Координированное комплектование может осуществляться на общегосударственном, региональном, местном, ведомственном уровнях.*

Корпоративная информационная система – информационная система, участниками которой может быть ограниченный круг лиц, определенный ее владельцем или соглашением участников этой информационной системы.

Криминалистическая идентификация – система научных положений (учение) о закономерностях криминалистического идентифицирования и разрабатываемых на основе этого специального криминалистического метода познания соответствующих рекомендаций, способов, средств, приемов и методик исследования и оценки криминалистически значимых объектов путем сопоставления их признаков и использования полученных результатов для раскрытия, расследования и предупреждения преступлений и судебного разбирательства.

Криминалистическая регистрация – система научных положений и разработанных на их основе методик по формированию и ведению цен-

трализованных оперативно-справочных, криминалистических, розыскных и иных учетов в целях информационного обеспечения раскрытия, расследования, предупреждения преступлений и решения других задач правоохранительных органов.

Криминалистические учеты (как разновидность криминалистических учетов ОВД) – учеты информационных центров, содержащие более подробные сведения об объекте учета и служащие для обеспечения мероприятий по установлению принадлежности утерянных (похищенных) и выявленных (изъятых) предметов, установлению личности неопознанных трупов, личности граждан, неспособных по состоянию здоровья или возрасту сообщить данные о себе.

Криминалистический учет – система хранения и поиска криминалистически значимой информации об объектах учета, пригодной для раскрытия и расследования преступлений.

Криминалистическое диагностирование – специальный криминалистический метод познания, суть которого состоит в исследовании и оценке объекта, имеющего определенную связь с событием расследуемого преступления, путем сопоставления его признаков с информацией (сведениями) об объектах из различных классификационных массивов (структур, систем, групп и т.п.), не имеющих заведомо известной (установленной, определенной) связи с событием расследуемого преступления; целью такого сопоставления является установление природы либо состояния объекта и использование полученных результатов в раскрытии, расследовании и предупреждении преступлений и судебном разбирательстве.

Криптографическая защита информации – защита информации с помощью ее криптографического преобразования.

Критерий выдачи – совокупность признаков, по которым определяется степень соответствия поискового образа документа поисковому предписанию и принимается решение о выдаче или невыдаче данного документа в ответ на информационный запрос.

Лингвистическая совместимость автоматизированных систем – частная совместимость АС, характеризуемая возможностью использования одних и тех же языковых средств общения персонала с комплексом средств автоматизации этих АС.

Лингвистическое обеспечение автоматизированной системы – совокупность средств и правил для формализации естественного языка, используемых при общении пользователей и эксплуатационного персонала АС с комплексом средств автоматизации при функционировании АС.

Лицензионные требования – совокупность требований, которые установлены положениями о лицензировании конкретных видов деятельности, основаны на соответствующих требованиях законодательства Рос-

сийской Федерации и направлены на обеспечение достижения целей лицензирования.

Лицензирование – деятельность лицензирующих органов по предоставлению, переоформлению лицензий, продлению срока действия лицензий в случае, если ограничение срока действия лицензий предусмотрено федеральными законами, осуществлению лицензионного контроля, приостановлению, возобновлению, прекращению действия и аннулированию лицензий, формированию и ведению реестра лицензий, формированию государственного информационного ресурса, а также по предоставлению в установленном порядке информации по вопросам лицензирования.

Лицензируемый вид деятельности – вид деятельности, на осуществление которого на территории Российской Федерации требуется получение лицензии в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», в соответствии с федеральными законами, регулирующими отношения в соответствующих сферах деятельности.

Лицо должностное органа, осуществляющего оперативно-розыскную деятельность – сотрудник оперативного подразделения, постоянно осуществляющий функции представителя власти, то есть наделенный правом в пределах своей компетенции предъявлять требования, а также принимать решения, обязательные для исполнения гражданами или предприятиями, учреждениями, организациями независимо от их ведомственной принадлежности и подчиненности.

Личный сыск – форма реализации совокупности диктуемых конкретными обстоятельствами ОРМ и методов ОРД, осуществляемых как гласно, так и негласно лично оперативными сотрудниками, в целях предупреждения, пресечения и раскрытия преступлений, розыска скрывшихся преступников и решения других задач ОРД.

Логическая организация данных – организация данных, учитывающая лишь те конструкции данных и операции над ними, которые находятся в распоряжении программы, использующей данные.

Макротезаурус – информационно-поисковый тезаурус, включающий лексические единицы высокой общности и покрывающий широкую область знания. *Используется для организации взаимодействия различных информационных систем.*

Маршрутизация данных – функция уровня взаимосвязи открытых систем, преобразующая наименование или адрес логического объекта уровня в маршрут для достижения этого объекта уровня.

Матрица доступа – таблица, отображающая правила разграничения доступа.

Межведомственная комиссия по защите государственной тайны – коллегиальный орган, координирующий деятельность федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных правовых актов и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне.

Межведомственное взаимодействие оперативно-розыскных органов – отношения оперативных работников различных ведомств, возникающие в связи с конкретными оперативными проверками на разных стадиях – от получения и оценки исходной информации до планирования и использования материального, оперативно-технического и силового обеспечения в реализации собранных данных (оперативно-тактического взаимодействия).

Межведомственное информационное взаимодействие – осуществляемое в целях предоставления государственных и муниципальных услуг взаимодействие по вопросам обмена документами и информацией, в том числе в электронной форме, между органами, предоставляющими государственные услуги, органами, предоставляющими муниципальные услуги, подведомственными государственным органам или органам местного самоуправления организациями, участвующими в предоставлении предусмотренных частью 1 статьи 1 Федерального закона «Об организации предоставления государственных и муниципальных услуг» государственных или муниципальных услуг, иными государственными органами, органами местного самоуправления, многофункциональными центрами.

Межведомственный запрос – документ на бумажном носителе или в форме электронного документа о представлении документов и информации, необходимых для предоставления государственной или муниципальной услуги, направленный органом, предоставляющим государственную услугу, органом, предоставляющим муниципальную услугу, либо многофункциональным центром в государственный орган, орган местного самоуправления, подведомственную государственному органу или органу местного самоуправления организацию, участвующую в предоставлении предусмотренных частью 1 статьи 1 Федерального закона «Об организации предоставления государственных и муниципальных услуг» государственных или муниципальных услуг, на основании запроса заявителя о предоставлении государственной или муниципальной услуги и соответствующий требованиям, установленным статьей 7.2 Федерального закона «Об организации предоставления государственных и муниципальных услуг».

Межведомственный электронный документооборот – взаимодействие информационных систем электронного документооборота федераль-

ных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации и иных государственных органов.

Межгосударственный розыск – комплекс оперативно-розыскных, поисковых, информационно-аналитических и иных мероприятий министерства внутренних дел, осуществляемых в соответствии с международными соглашениями и национальным законодательством с использованием межгосударственного информационного банка и направленных на обнаружение в целях последующего ареста или предоставления информации обо всех категориях разыскиваемых, находящихся за пределами государства – инициатора розыска, но в пределах территории государства – участника СНГ.

Метод доступа – совокупность соглашений и средств, с помощью которых реализуется заданный вид доступа к физическим записям набора данных. *В зависимости от вида доступа и организации набора данных в конкретных системах обработки данных различают, например, последовательные, прямые, иерархические методы доступа.*

Метод оперативно-розыскной деятельности – совокупность приемов и способов, применяемых для решения оперативно-тактических задач в процессе тактической реализации ОРМ.

Методы и средства гласные – способы собирания информации, которые позволяют использовать результаты, полученные в ходе проведения ОРМ, в уголовном судопроизводстве.

Методы оперативно-розыскной деятельности – социально апробированные приемы и способы познания окружающей среды в деятельности по предупреждению и раскрытию преступлений, собиранию оперативно-розыскной информации.

Микротезаурус – специализированный информационно-поисковый тезаурус небольшого объема, составленный на основе развития выборки из более полного информационно-поискового тезауруса и дополнительно включающий конкретные узкие понятия определенной тематики.

Мимика – движение мышц и элементов лица, меняющих его выражение в зависимости от эмоционального состояния человека или его желания. *Она может быть очень развитой или маловыразительной. Обычно отмечают наиболее выраженную и привычную мимику (поднятие бровей, закусывание губ, подмигивание и т.п.).*

Многомерная классификация – классификационная система, в которой каждый класс может разделяться более чем по одному признаку.

Многоуровневая защита – класс систем, содержащих информацию различной степени чувствительности, доступ к которым открыт для пользователей с различными правами доступа к информации и потребностями, но предотвращается для тех групп пользователей, которые не имеют на это

прав. *Многоуровневая защита является защитой компьютера, а не его надежностью, относящейся к предотвращению неисправности оборудования или ошибки оператора.*

Модель данных – совокупность правил порождения структур данных в базе данных, операций над ними, а также ограничений целостности, определяющих допустимые связи и значения данных, последовательность их изменения. *Для задания модели данных используется язык описания данных и язык манипулирования данными.*

Модель защиты – абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа.

Модель нарушителя правил разграничения доступа – абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации. *Видом описательного представления свойств или характеристик угроз безопасности информации может быть специальный нормативный документ.*

Мониторинг безопасности информации – постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

Наведение справок – получение информации, необходимой для решения задач оперативно-розыскной деятельности, из оперативных, криминалистических и иных баз данных (учетов), информационных систем, от юридических и физических лиц, а также из других источников.

Нарушитель правил разграничения доступа – субъект доступа, осуществляющий несанкционированный доступ к информации.

Нейронная ЭВМ – вычислительное устройство, разработанное или модифицированное для имитации поведения нейрона или совокупности нейронов, например, вычислительное устройство, характеризуемое способностью аппаратуры модулировать вес и количество взаимных связей множества вычислительных компонентов на основе предыдущей информации.

Неправомерный доступ – несанкционированное обращение к компьютерной информации.

Несанкционированное воздействие на информацию – воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтоже-

нию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. *Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.*

Несанкционированный доступ к программным средствам – доступ к программам, записанным в памяти ЭВМ или на машинном носителе, а также отраженным в документации на эти программы, осуществленный с нарушением установленных правил.

Номенклатура дел – систематизированный перечень наименований дел, заводимых в организации, с указанием сроков их хранения, оформленный в установленном порядке.

Нормативно-справочная информация автоматизированной системы – информация, заимствованная из нормативных документов и справочников и используемая при функционировании АС.

Носители сведений, составляющих государственную тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обеспечение режима секретности – деятельность компетентных органов по созданию и применению системы мер административно-правовых режимов, обеспечивающих защиту государственной и служебной тайны. *В ОРД возлагается на руководителей оперативных аппаратов в целях сохранения в тайне сведений о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках, о лицах, оказывающих содействие, а также об организации, тактике, методах и средствах ОРД.*

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации (без использования таких средств), с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступные (открытые) информационные системы – информационные системы, доступ к которым не ограничен законом.

Объединенный архивный фонд – архивный фонд, сформированный из документов двух или более фондообразователей, имеющих между собой исторически обусловленные связи.

Объектографическая база данных – база первичных данных, запись в которой содержит данные об отдельном объекте предметной области.

Объем документооборота – количество документов, поступивших в организацию и созданных ею за определенный период.

Оперативная комбинация – комплекс действий, объединенных единым замыслом, легендой и направленных на решение конкретной задачи обнаружения, предотвращения или раскрытия преступления (многоцелевой способ действия, эффективно применяемый во всех сферах ОРД).

Оперативное подразделение – подразделение, непосредственно осуществляющее оперативно-розыскную деятельность в пределах определенной ведомственными нормативными актами компетенции.

Оперативно-розыскная деятельность (ОРД) – вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то ФЗ об ОРД, в пределах их полномочий посредством проведения ОРМ в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.

Оперативно-розыскная информация – разновидность социальной информации, специфичной по цели получения (борьба с преступностью), методам получения и режиму использования, обеспечивающему конспирацию, надежную зашифровку источников, возможность проверки сообщаемых сведений и их применение только заинтересованными работниками.

Оперативно-розыскное мероприятие (ОРМ) – совокупность гласных и негласных действий должностных лиц органов, уполномоченных на то законом, по получению, фиксации и оценке информации, представляющей интерес для решения задач оперативно-розыскной деятельности.

Оперативно-справочные учеты – учеты информационных центров, предназначенные для предупреждения, раскрытия и расследования преступлений, путем подтверждения наличия (или отсутствия) сведений о привлечении лица к уголовной ответственности, о судимости, реабилитации, времени и месте отбывания наказания; установления местонахождения разыскиваемых лиц; установления личности граждан.

Оперативно-тактическая ситуация – реально существующее на данный момент состояние криминального события (или иного связанного с ним факта) либо угрозы наступления такого события, по поводу которого

осуществляется ОРМ, условия, в которых приходится действовать оперуполномоченному, его возможности принять необходимые меры, формулируемые в виде конкретной задачи.

Опознавательная съемка – воспроизведение средствами фотографии внешних признаков лиц, совершивших преступление, неопознанных трупов с целью их последующего опознания, регистрации в криминалистических учетах и розыска преступников.

Орган, осуществляющий оперативно-розыскную деятельность – уполномоченное законодателем на проведение ОРМ оперативное подразделение одного из федеральных государственных органов, перечисленных в статье 13 ФЗ об ОРД.

Организация проведения оперативно-розыскных мероприятий – разновидность специальной управленческой деятельности, состоящая в планировании конкретных ОРМ, оптимальной реализации принятых по их проведению решений, контроле за их исполнением и т.д. с учетом складывающейся оперативной обстановки.

Органы, осуществляющие регистрационную деятельность в ОВД – информационные центры и экспертно-криминалистические центры ГУ МВД, УМВД областей, краев, МВД республик. *Головными учреждениями выступают Главный информационно-аналитический центр и Экспертно-криминалистический центр МВД России.*

Основания для проведения ОРМ – фактические данные, достаточные для предположения о совершении деяния, подпадающего под признаки того или иного состава преступления, либо о событиях или действиях, которые могут представлять угрозу государственной, военной, экономической или экологической безопасности Российской Федерации.

Открытый ключ электронной цифровой подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе.

Отождествление личности – установление и идентификация личности интересующего органы внутренних дел лица, осуществляемые с помощью неизменяемых признаков человека.

Отсылочная база данных – база данных, отсылающая пользователя к другим источникам для получения полной или дополнительной информации.

Охраняемые сведения – сведения, составляющие государственную или иную охраняемую законом тайну.

Оценка безопасности – исследования (испытания), проводимые для проверки соответствия профиля защиты, задания по безопасности или изделия информационной технологии установленным требованиям безопасности.

Оценка информационного риска – общий процесс анализа информационного риска и его оценивания.

Оценка соответствия требованиям по защите информации – прямое или косвенное определение степени соблюдения требований по защите информации, предъявляемых к объекту защиты информации.

Оценка уровня причинения ущерба или вреда вследствие невыполнения требований технических регламентов – учет и анализ всех случаев причинения ущерба имуществу физических или юридических лиц, государственному или муниципальному имуществу, вреда для жизни или здоровья граждан, животных и растений, вреда окружающей среде вследствие нарушения требований технических регламентов с учетом тяжести этого ущерба и вреда.

Пакетный поиск – автоматизированный информационный поиск, при котором информационные запросы накапливаются в специальном массиве для последующей совместной обработки.

Параметр схемы электронной цифровой подписи – элемент данных, общий для всех субъектов схемы цифровой подписи, известный или доступный всем этим субъектам.

Переработка (модификация) программы для ЭВМ или базы данных – любые их изменения, в том числе перевод такой программы или такой базы данных с одного языка на другой язык, за исключением адаптации, то есть внесения изменений, осуществляемых исключительно в целях функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя.

Перечень сведений, составляющих государственную тайну – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Персональные данные – информация (зафиксированная на материальном носителе) о конкретном человеке, которая отождествлена или может быть отождествлена с ним. *К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие.*

Персональные данные категории 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов,

религиозных и философских убеждений, состояния здоровья, интимной жизни.

Персональные данные категории 2 – персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Персональные данные категории 3 – персональные данные, позволяющие идентифицировать субъекта персональных данных.

Персональные данные категории 4 – обезличенные и (или) общедоступные персональные данные.

Подлинный документ – документ, сведения об авторе, времени и месте создания которого, содержащиеся в самом документе или выявленные иным путем, подтверждают достоверность его происхождения.

Подписка о неразглашении – письменное обязательство о сохранении подписывающим лицом в тайне ставших ему известными сведений. В ОРД отбирается, например, у лиц, оказывающих помощь при проведении отдельных ОРМ.

Подписывающее лицо – физическое или юридическое лицо, создающее электронную цифровую подпись на электронных данных – владелец закрытого ключа электронной цифровой подписи или его представитель, которому доверен закрытый ключ электронной цифровой подписи.

Подразделение оперативное – отделение (группа), отдел, служба, управление, главное управление, а равно подразделение собственной безопасности и иное организационно-штатное подразделение, являющееся структурным звеном оперативно-розыскного органа, в функциональные обязанности которого входит решение задач, предусмотренных ФЗ об ОРД.

Подтверждение подлинности электронной цифровой подписи в электронном документе – положительный результат проверки соответствующим сертифицированным средством электронной цифровой подписи с использованием сертификата ключа подписи принадлежности электронной цифровой подписи в электронном документе владельцу сертификата ключа подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе.

Поиск оперативный – одна из форм ОРД, предназначенная для обнаружения необходимой информации, выявления интересующих объектов, материалов, изделий, а также лиц, от которых, судя по их противоправному поведению, можно ожидать совершения преступлений.

Поисковая команда – операция при информационном поиске, имеющая целью выявление определенной части информации в поисковом массиве.

Поисковое предписание – текст, включающий поисковый образ запроса и указания о логических операциях, подлежащих выполнению в процессе информационного поиска.

Поисковый образ – текст, состоящий из лексических единиц информационно-поискового языка, выражающий содержание документа или информационного запроса и предназначенный для реализации информационного поиска.

Поисковый образ документа – поисковый образ, выражающий основное смысловое содержание документа.

Поисковый образ запроса – поисковый образ, выражающий смысловое содержание информационного запроса.

Поисковый термин – лексическая единица информационно-поискового языка, являющаяся элементом поискового образа запроса, наличие которой в поисковом образе документа служит основанием для выдачи документа по данному информационному запросу.

Поисковый шум – совокупность выданных при информационном поиске нерелевантных документов.

Показатель защищенности средств вычислительной техники – характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники.

Показатель эффективности защиты информации – мера или характеристика для оценки эффективности защиты информации.

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Полнота индексирования – степень отражения в поисковом образе аспектов содержания документа и (или) запроса. *Определяется как отношение числа специфических терминов и фактографических сведений, включенных в поисковый образ, к числу таковых терминов и сведений в тексте документа или запроса.*

Полнотекстовая база данных – текстовая база первичных данных, содержащая полные тексты документов.

Полнотекстовый поиск – автоматизированный документальный поиск, при котором в качестве поискового образа документа используется его полный текст или существенные части текста.

Получатель документов – юридическое лицо или его структурное подразделение, наделенные правом получения, хранения и общественного использования обязательного экземпляра на безвозмездной основе.

Пользователь архивными документами – государственный орган, орган местного самоуправления либо юридическое или физическое лицо, обращающиеся на законных основаниях к архивным документам для получения и использования необходимой информации.

Попутная информация – информация, изначально не имеющая отношения к расследуемым событиям или действиям, однако в процессе ее сопоставления возможно получение новых данных, обоснованных предположений, выводов, выдвижение версий, которые требуют проверки, а соответственно, и проведения дополнительных ОРМ.

Поручение (следователя, органа дознания) – одно из оснований для проведения оперативным подразделением каких-либо ОРМ, состоящее в документально оформленном (в соответствии с уголовно-процессуальным законодательством) задании следователя (органа дознания) о проведении необходимых оперативно-розыскных мероприятий по уголовному делу, находящемуся в его производстве.

Потребитель информации – лицо или коллектив, получающие и использующие информацию в практической деятельности.

Походка – совокупность привычных автоматических движений при ходьбе как проявление сформировавшегося у человека определенного динамического стереотипа. *Это обстоятельство определяет постоянство таких элементов походки, как длина шага (левого, правого), ширина шага, угол шагов, угол разворота стопы. При описании походки отмечают размер шага (длинный, короткий), ширину шага, темп, вид. Отмечается также хромота, иные нарушения походки, положение рук при ходьбе. Походка может изменяться под влиянием заболеваний ног, нервной системы, травм головы.*

Правила (нормы) стандартизации – нормативный документ, устанавливающий обязательные для применения организационно-методические положения, которые дополняют или конкретизируют отдельные положения основополагающего национального стандарта и определяют порядок и методы выполнения работ по стандартизации.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Правило доступа к защищаемой информации – совокупность правил, устанавливающих порядок и условия доступа субъекта к защищаемой информации и ее носителям.

Право доступа к защищаемой информации – совокупность правил доступа к защищаемой информации, установленных правовыми документами или собственником, владельцем информации.

Правовая защита информации – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Правовая и социальная защита участников ОРД – совокупность (система) и конечные результаты реализации предусмотренных законом и подзаконными правовыми актами целевых мер, осуществляемых государственными органами – субъектами ОРД в целях обеспечения прав и законных интересов должностных лиц ОРД и лиц, оказывающих им содействие, создание благоприятных условий для их эффективного участия в решении задач ОРД, а также возмещение причиненного им вреда.

Предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Предотвращение перехвата техническими средствами информации, передаваемой по каналам связи – достигается применением криптографических и иных методов и средств защиты, а также проведением организационно-технических и режимных мероприятий.

Предотвращение перехвата техническими средствами речевой информации из помещений и объектов – деятельность, осуществляемая с применением специальных средств защиты, с разработкой проектных решений, обеспечивающих звукоизоляцию помещений, с выявлением специальных устройств подслушивания и с другими организационными и режимными мероприятиями.

Предотвращение специальных программно-технических воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации – деятельность, осуществляемая с применением специальных программных и аппаратных средств защиты (антивирусных процессоров, антивирусных программ), с организацией системы контроля безопасности программного обеспечения.

Предотвращение утечки обрабатываемой информации за счет побочных электромагнитных излучений и наводок, а также электроакустических преобразований – деятельность, осуществляемая с применением защищенных технических средств, аппаратных средств защиты, средств активного противодействия, экранированием зданий или отдель-

ных помещений, установлением контролируемой зоны вокруг средств информатизации и другими организационными и техническими мерами.

Представление данных – характеристика, выражающая правила кодирования элементов и образования конструкций данных на конкретном уровне рассмотрения в вычислительной системе.

Признаки внешности – воспринимаемые зрительно характеристики внешнего облика в целом или отдельных его элементов, с помощью которых можно отличить (узнать) человека или отнести его к определенной группе людей. *Подразделяются на анатомические (наблюдаемые признаки наружного строения тела и лица), функциональные (заметные признаки привычного состояния человека и его действий) и сопутствующие (признаки вещей, находящихся в пользовании человека).*

Проверка подлинности электронной цифровой подписи – последовательность действий, при которой лицо, получившее электронное сообщение, подписанное электронной цифровой подписью, и открытый ключ подписавшего лица, может определить, было ли это сообщение подписано с использованием закрытого ключа, соответствующего открытому ключу подписавшего лица, и были ли изменены исходные данные после создания электронной цифровой подписи.

Программная закладка – преднамеренно внесенный в программное обеспечение функциональный объект, который при определенных условиях инициирует реализацию недекларированных возможностей программного обеспечения.

Протокол – официальный документ, в котором фиксируются какие-либо фактические обстоятельства. В деятельности ОВД РФ могут составляться протоколы следственных действий, протоколы об административных правонарушениях.

Процесс проверки подписи – процесс, в качестве исходных данных которого используются подписанное сообщение, ключ проверки и параметры схемы ЭЦП и результатом которого является заключение о правильности или ошибочности цифровой подписи.

Процесс формирования подписи – процесс, в качестве исходных данных которого используются сообщение, ключ подписи и параметры схемы ЭЦП, а в результате формируется цифровая подпись.

Рабочая документация на автоматизированную систему – комплект проектных документов на АС, содержащий взаимоувязанные решения по системе в целом, ее функциям, всем видам обеспечения АС, достаточные для комплектации, монтажа, наладки и функционирования АС, ее проверки и обеспечения работоспособности.

Разведка инициативная – сбор информации о криминально опасных лицах, а также фактах, изучение которых необходимо для предупреждения противоправной деятельности.

Разведка профилактическая – наблюдение с целью сбора данных о лицах, представляющих оперативный интерес, для своевременного распознания их преступных замыслов и принятия к ним мер профилактического характера.

Разведывательно-поисковый характер ОРД – особая характеристика ОРД, отражающая сочетание гласных и негласных методов и средств в процессе ее осуществления.

Разглашение государственной тайны – разглашение сведений, составляющих государственную тайну, лицом, которому она была доверена или стала известна по службе или работе, если эти сведения стали достоянием других лиц, при отсутствии признаков государственной измены (статья 283 УК РФ).

Разграничение доступа – разделение доступа должностных лиц к данным в соответствии с имеющимися разрешениями.

Раскрытие преступлений – одна из задач ОРД, связанная с обнаружением противоправных действий и лиц, их совершивших. Осуществляется в рамках дел оперативного учета с использованием комплекса ОРМ.

Распознавание лиц – раздел биометрики, представляющий методы и средства решения задач распознавания и наблюдения человека (идентификацию и классификацию) по изображениям его лица, а также интерпретации действий человека – его намерений и поведения – через идентификацию его эмоционального состояния и окружающих его людей.

Распределенная база данных – совокупность баз данных, физически распределенная по взаимосвязанным ресурсам вычислительной системы и доступная для совместного использования в различных приложениях.

Регистрационное свидетельство на открытый ключ электронной цифровой подписи – документ, подтверждающий соответствие этого открытого ключа электронной цифровой подписи закрытому ключу, выданный центром регистрации открытых ключей владельцу закрытого ключа электронной цифровой подписи или его полномочному представителю.

Регистрационный индекс документа – цифровое или буквенно-цифровое обозначение, присваиваемое документу при его регистрации.

Регистрация криминалистическая – система криминалистического учета определенных объектов, используемая для раскрытия и расследования преступлений. *По способу обработки и выдачи регистрируемых данных различают ручные, механизированные и автоматизированные системы учета. По форме учета – картотеки, списки, альбомы, коллекции. По способу учета – алфавитные, дактилоскопические, по признакам*

внешности, по способу совершения преступления, по описанию и вещественным отображениям регистрируемых объектов. По виду учетов подразделяются на оперативно-справочные, оперативно-розыскные системы и коллекции. В настоящее время широкое применение находят автоматизированные информационно-поисковые системы (АИПС). Условно термин «регистрация криминалистическая» иногда употребляется для обозначения всей совокупности криминалистического учета.

Режим пакетной обработки – режим выполнения совокупности задач, при котором все они выполняются системой обработки информации в основном автоматически без синхронизации с событиями вне этой СОИ, в частности, без связи с лицами, представившими задание для выполнения.

Режим реального времени – режим обработки информации, при котором обеспечивается взаимодействие системы обработки информации с внешними по отношению к ней процессами в темпе, соизмеримом со скоростью протекания этих процессов.

Резервирование – способ обеспечения надежности объекта за счет использования дополнительных средств и (или) возможностей, избыточных по отношению к минимально необходимым для выполнения требуемых функций.

Резервирование без восстановления – резервирование, при котором восстановление отказавших основных и (или) резервных элементов технически невозможно без нарушения работоспособности объекта в целом и (или) не предусмотрено эксплуатационной документацией.

Резервирование замещением – резервирование, при котором функции основного элемента передаются резервному только после отказа основного элемента.

Резервирование с восстановлением – резервирование, при котором восстановление отказавших основных и (или) резервных элементов технически возможно без нарушения работоспособности объекта в целом и предусмотрено эксплуатационной документацией.

Резервируемый элемент – основной элемент, на случай отказа которого в объекте предусмотрены один или несколько резервных элементов.

Результаты оперативно-розыскной деятельности – сведения, полученные в соответствии с ФЗ об ОРД о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда.

Рекомендации по стандартизации – документ, содержащий советы организационно-методического характера, которые касаются проведения работ по стандартизации и способствуют применению основополагающего

национального стандарта или содержат положения, которые целесообразно предварительно проверить на практике до их установления в основополагающем национальном стандарте.

Релевантность – соответствие полученной информации информационному запросу.

Реляционная база данных – база данных, реализованная в соответствии с реляционной моделью данных.

Реляционная модель данных – модель данных, основанная на представлении данных в виде набора отношений, каждое из которых представляет собой подмножество декартова произведения определенных множеств, и манипулировании ими с помощью множества операций реляционной алгебры или реляционного исчисления.

Ретроспективный поиск – информационный поиск по разовым информационным запросам в ранее накопленном информационном массиве.

Розыск – деятельность правоохранительных органов (следователей, органов дознания и иных компетентных органов) по установлению места нахождения обвиняемых, скрывшихся от следствия и суда, а также от отбывания наказания, и без вести пропавших граждан.

Розыскная ориентировка – краткое описание особенностей внешнего облика человека, при составлении которого выделяют и описывают признаки внешности, главным образом, резко отличающиеся от общераспространенных.

Розыскные меры – меры, принимаемые дознавателем, следователем, а также органом дознания по поручению дознавателя или следователя для установления лица, подозреваемого в совершении преступления.

Розыскные учеты – учеты информационных центров, содержащие более подробные сведения об объекте учета и служащие для обеспечения мероприятий регионального, федерального и межгосударственного розыска похищенных предметов, скрывшихся лиц.

Российская национальная стандартизация – деятельность по установлению правил и характеристик в целях их добровольного многократного использования, направленная на достижение упорядоченности в сферах производства и обращения продукции и повышение конкурентоспособности продукции, работ или услуг.

Санкционированный доступ к информации – доступ к информации, не нарушающий правила разграничения доступа.

Сбор образцов для сравнительного исследования – следственное действие, заключающееся в изъятии и сохранении предметов, объектов и веществ, а также других образцов с целью выявления их особенностей и признаков для последующего сравнительного исследования.

Свободный доступ к информации – предоставление пользователям информации – гражданам, юридическим лицам, органам государственной власти и управления, органам регионального и местного самоуправления, общественным объединениям государств – участников Соглашения о свободном доступе и порядке обмена открытой научно-технической информацией государств – участников СНГ – права на открытую информацию, которое предусматривает возможность свободного ее получения, хранения, использования и распространения при осуществлении научной, научно-технической, производственной, общественной и иной деятельности, не запрещенной действующим национальным законодательством.

Семейство профилей защиты – совокупность упорядоченных взаимосвязанных профилей защиты, которые относятся к определенному типу изделий информационной технологии.

Сертификат защиты – документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

Сертификат ключа подписи – документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сертификат соответствия – документ, выдаваемый в соответствии с правилами сертификации, указывающий, что обеспечивается необходимая уверенность в том, что должным образом идентифицированная продукция, процесс или услуга соответствуют конкретному стандарту или другому нормативному документу.

Сертификат средств электронной цифровой подписи – документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям.

Сертификация – процедура подтверждения соответствия технических и программных средств, посредством которой независимая от изготовителя (продавца, исполнителя) и потребителя (покупателя) организация

устанавливает в письменной форме соответствие продукции установленным требованиям.

Сертификация на соответствие требованиям по безопасности информации – форма осуществляемого органом по сертификации подтверждения соответствия объектов оценки требованиям по безопасности информации, установленным техническими регламентами, стандартами или условиями договоров.

Сертификация соответствия – действие третьей стороны, доказывающее, что обеспечивается необходимая уверенность в том, что должным образом идентифицированная продукция, процесс или услуга соответствуют конкретному стандарту или другому нормативному документу.

Сертификация средств защиты информации по требованиям безопасности информации – деятельность по подтверждению их соответствия требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией России).

Сертификация уровня защиты – процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите.

Силы оперативно-розыскной деятельности – собирательное понятие для обозначения группы людей, возможности которых используются при осуществлении ОРМ.

Симультанное опознание – отнесение воспринимаемого предмета к какому-либо классу одномоментно, как мгновенное «схватывание».

Синкретическое восприятие – восприятие, характеризующееся схематичностью и слитностью структуры, когда выделяются лишь общие контуры воспринимаемого объекта, без анализа его частей и свойств. *Синкретическое восприятие наблюдается у детей, у инфантильных малоопытных людей. Синкретизм вызывает неадекватность восприятия. При таком восприятии предмет в сознании не появляется в специфических, присущих ему особенностях и может рассматриваться как другой предмет, который чем-то напоминает воспринимаемое*.

Система гарантий законности при проведении ОРМ – система юридических средств (правовые акты, юридическая ответственность, контрольно-надзорная деятельность и др.), при помощи которых обеспечивается строгое и неуклонное соблюдение законности в сфере ОРД.

Система межведомственного электронного взаимодействия (СМЭВ) – государственная информационная система, обеспечивающая типовые механизмы взаимодействия информационных систем, используемых при предоставлении государственных (муниципальных) услуг и ис-

полнении государственных (муниципальных) функций, с применением электронных сервисов со стандартизированными интерфейсами (сервис-ориентированная архитектура).

Система обработки информации – совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, обеспечивающая выполнение автоматизированной обработки информации.

Система разграничения доступа – совокупность реализуемых правил разграничения доступа в средствах вычислительной техники или автоматизированных системах.

Система управления базами данных (СУБД) – совокупность программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных.

Система электронного документооборота – информационная система, обеспечивающая сбор документов (включение документов в систему), их обработку, управление документами и доступ к ним.

Скрипт – программа, которая может сопровождать документ HTML или быть непосредственно внедренной в него. *Эта программа выполняется на персональном компьютере пользователя при загрузке документа или в другое время, например, когда активизируется ссылка. Скрипты используются для усиления интерактивности документов HTML. В частности, скрипты могут выполняться во время загрузки документа и динамически изменять содержимое документа.*

Скульптурный портрет – одна из форм передачи признаков внешности, получаемая путем пластической реконструкции лица по черепу (метод профессора М.М. Герасимова). *Этот метод позволяет передать комплекс признаков внешности, различных по своей природе: объективных, относительно объективных и субъективных. По этой причине С.п., воссозданные по черепу, также не могут быть объектом, предъявляемым для опознания.*

Словесный портрет – криминалистический метод описания внешности человека с использованием единых терминов, осуществляемый по определенной системе в целях уголовной регистрации, розыска и отождествления живых лиц и трупов. *Правила описания по методу словесного портрета базируются на взаимосвязанных принципах системности и полноты. Принцип системности определяет последовательность (очередность) описания. Принцип полноты предусматривает подробную характеристику.*

Составной портрет – изображение лица разыскиваемого подозреваемого или потерпевшего, составленное по показаниям очевидцев, рисованное или составленное с использованием специальных технических средств (фоторобот, идентификационный комплект рисунков и др.).

Социальная и правовая защита должностных лиц органов, осуществляющих оперативно-розыскную деятельность – распространение гарантии социальной и правовой защиты на должностных лиц органов, осуществляющих ОРД.

Сочетание гласных и негласных методов и средств – принцип ОРД, выработанный оперативно-розыскной практикой, проявляющийся в осуществлении открытых методов, заимствованных из криминалистики и других наук, для легализации информации, полученной в процессе применения тайных разведывательно-поисковых мероприятий, осуществляемых в интересах решения задач ОРД.

Специальная проверка – проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств.

Справка – документ, содержащий сведения о результатах проведения ОРМ.

Среда безопасности – область среды, в пределах которой предусматривается обеспечение необходимых условий для поддержания требуемого режима безопасности изделия информационной технологии.

Среднее время преодоления защиты – математическое ожидание времени выполнения несанкционированных действий по преодолению защиты до получения доступа к данным.

Среднее число действий по преодолению защиты – математическое ожидание числа несанкционированных действий по преодолению защиты до получения доступа к данным.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации.

Средства ОРД – совокупность научно-технических, информационных и боевых систем, применяемых в целях решения задач ОРД и обеспечения безопасности самих сотрудников оперативных аппаратов.

Средство криптографической защиты информации – средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Структурированный язык запросов SQL – декларативный язык программирования, применяемый для создания, модификации и управления данными в реляционной базе данных, управляемой соответствующей системой управления БД. *SQL принят в качестве стандарта языка ком-*

муникации реляционных БД. Конкретные реализации SQL несколько отличаются друг от друга и используют расширение стандарта. Типы команд SQL: язык определения данных, язык манипулирования данными, язык запросов, язык управления данными. В SQL задействованы команды администрирования данных, команды управления транзакциями. Команды определения данных используются для определения структур БД, позволяют создавать, изменять, удалять таблицы. Команды манипулирования данными используются для манипулирования информацией внутри объектов реляционной БД. Язык запросов служит для выборки данных. Это наиболее известный язык для разработчиков БД. Язык управления данными позволяет управлять доступом к информации, находящейся в БД. Команды администрирования данных позволяют осуществлять контроль за действиями, выполняемыми пользователями, могут использоваться для анализа производительности системы. Команды управления транзакциями используются для сохранения результатов транзакции, отмены результатов транзакции, создания внутри транзакции точек отката.

Субъективный портрет – изображение лица или фигуры человека, в той или иной степени соответствующее представлению очевидца о внешнем облике изображенного, изготовленное с помощью специальных методов и соответствующих технических средств.

Судебная видеозапись – система научных положений, технических средств, методов и приемов, используемых при изготовлении, демонстрации и хранении видеофильмов с целью предупреждения, выявления, расследования, раскрытия преступлений и рассмотрения уголовных дел в суде.

Судебная фотография – вспомогательное средство фиксации доказательств.

Сукцессивное опознание – отнесение воспринимаемого предмета к какому-либо классу в результате развернутого анализа его признаков.

Схема базы данных – описание базы данных в контексте конкретной модели данных.

Тайна связи – тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, не подлежащая разглашению без согласия пользователя услуг почтовой связи.

Текстовая база данных – база данных, записи в которой содержат (главным образом) текст на естественном языке.

Теория оперативно-розыскной деятельности – отрасль научного знания о закономерностях возникновения фактических данных, отражающих подготовку и совершение неочевидных преступлений, об организации и тактике выявления таких данных с использованием возможностей ОРД в установленных правовых рамках для последующей реализации в целях борьбы с преступностью.

Терминология оперативно-розыскная официальная – совокупность слов и выражений, обозначающих определенные понятия, употребляемых законодателем в области ОРД, в также используемых в нормативных правовых актах федеральных органов государственной власти и в ведомственных нормативных актах правоохранительных органов и специальных служб.

Техническая защита информации – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Техническая защита конфиденциальной информации – комплекс мероприятий и (или) услуг по защите ее от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на нее в целях уничтожения, искажения или блокирования доступа к ней.

Технические средства для выявления электронных устройств, предназначенных для негласного получения информации – специальная и контрольно-измерительная аппаратура, а также средства вычислительной техники, позволяющие осуществлять поиск электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах.

Технические средства, позволяющие осуществлять обработку персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Технический регламент – документ, который принят международным договором Российской Федерации, ратифицированным в порядке, установленном законодательством Российской Федерации, или межправительственным соглашением, заключенным в порядке, установленном законодательством Российской Федерации, или федеральным законом, или указом Президента Российской Федерации, или постановлением Правительства Российской Федерации, или нормативным правовым актом федерального органа исполнительной власти по техническому регулированию и устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям или к связанным с требованиями к продукции

процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации).

Удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Узнавание – опознание воспринимаемого объекта по прошлому опыту. *Основой У. служит сличение наличного восприятия со следами, сохранившимися в памяти. У. может быть произвольным, когда оно используется для запоминания или заучивания, и непроизвольным, когда не стоит специальная задача. При этом У. может быть неполным, неопределенным, фантомным, когда переживается чувство «знакомости» в отношении объекта, которого на самом деле никогда не встречал. Это явление носит название парамнезии.*

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Управление данными – совокупность функций обеспечения требуемого представления данных, их накопления и хранения, обновления, удаления, поиска по заданному критерию и выдачи данных.

Управление потоком данных – регулирование потока данных внутри или между смежными уровнями взаимосвязи открытых систем.

Уровень полномочий субъекта доступа – совокупность прав доступа субъекта доступа.

Уровень представления данных – уровень взаимосвязи открытых систем, обеспечивающий услуги по обмену данными между логическими объектами прикладного уровня, преобразование и представление данных в нужном формате.

Участники электронного взаимодействия – осуществляющие обмен информацией в электронной форме государственные органы, органы местного самоуправления, организации, а также граждане.

Фактографическая информационно-поисковая система – информационно-поисковая система, предназначенная для поиска фактов.

Фактографическая справка – ответ на запрос, содержащий фактические сведения.

Фактографический информационно-поисковый язык – информационно-поисковый язык, предназначенный для индексирования описаний фактов и информационного поиска в фактографических информационных массивах.

Фактографическое индексирование – индексирование, предусматривающее отражение в поисковом образе документа конкретных сведений (фактов).

Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Формирование ИС ОРИ – комплекс мероприятий, направленных на получение, обработку, хранение, структурирование оперативно-розыскной информации, организацию доступа к различным источникам – информационным ресурсам, в том числе и из открытых источников, которые позволяют осуществлять мероприятия, относящиеся к задачам ОРД, конечной целью которых является раскрытие и профилактика преступлений.

Фототека – организация или служба (отдел библиотеки), в обязанность которой входит сбор, хранение и предоставление в распоряжение пользователей фотографических документов.

Функциональные признаки внешности – признаки внешнего облика, проявляющиеся в процессе жизнедеятельности человека, характеризующие его двигательные и физиологические функции (жестикуляция, мимика и т.п.).

Хранение архивных документов – обеспечение рационального размещения и сохранности документов.

Хэш-функция – функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам: 1) по данному значению функции сложно вычислить исходные данные, отображенные в это значение; 2) для заданных исходных данных трудно найти другие исходные данные, отображаемые с тем же результатом; 3) трудно найти какую-либо пару исходных данных с одинаковым значением хэш-функции. *Применительно к области ЭЦП свойство 1 подразумевает, что по известной ЭЦП невозможно восстановить исходное сообщение; свойство 2 подразумевает, что для заданного подписанного сообщения трудно подобрать другое (фальсифицированное) сообщение, имеющее ту же ЭЦП, свойство 3 подразумевает, что трудно подобрать какую-либо пару сообщений, имеющих одну и ту же подпись.*

Центр регистрации отрытого ключа электронной цифровой подписи – юридическое лицо, обладающее правомочиями на удостоверение соответствия открытого ключа электронной цифровой подписи закрытому

ключу лица, на имя которого выдано регистрационное свидетельство (владелец свидетельства).

Человеко-машинный интерфейс – периферийные устройства, внесенные в каталог производителя и снабженные кнопками, световыми индикаторами, клавиатурой, дисплеями или эквивалентными устройствами и служащие интерфейсом оператору, как, например, пульт управления (мониторинга) мотором, интерфейс оператора общего назначения.

Численно-текстовая база данных – база данных, содержащая числовые данные и текстовую информацию.

Числовая база данных – база данных, содержащая числовые данные.

Шифровальные средства – а) реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для защиты информации (в том числе входящие в системы и комплексы защиты информации от несанкционированного доступа – НСД), циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику; б) реализующие криптографические алгоритмы преобразования информации аппаратные, программные и аппаратно-программные средства, системы и комплексы защиты от навязывания ложной информации, включая средства имитозащиты и «электронной подписи»; в) аппаратные, программные и аппаратно-программные средства, системы и комплексы, предназначенные для изготовления и распределения ключевых документов, используемых в шифровальных средствах, независимо от вида носителя ключевой информации.

Экспертно-криминалистические учеты – учеты экспертно-криминалистических подразделений, содержащие более подробные сведения об объекте учета и служащие для обеспечения мероприятий по идентификации предметов, оставивших следы на месте происшествия, установлению личности человека по оставленным им следам, признакам внешности, голоса, костным останкам.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронная цифровая подпись (ЭЦП) – реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах.

Электронный документооборот – документооборот с применением информационной системы.

Электронный паспорт федеральной государственной информационной системы – электронный документ, подтверждающий регистрацию федеральной государственной информационной системы в реестре.

Язык ключевых слов – информационно-поисковый язык, предназначенный для индексирования документов и информационных запросов посредством ключевых слов.

Язык манипулирования данными – язык, предназначенный для формулирования запросов на поиск, обмен данными между прикладной программой и базой данных, а также для расширения языка программирования либо как самостоятельный язык.

Язык описания данных – язык, предназначенный для описания схем баз данных.

Список литературы

1. О государственной тайне: закон Российской Федерации от 21 июля 1993 г. № 5485-1: ред. от 29 июля 2018 г. // Собр. законодательства Рос. Федерации. 1997. № 41. С. 8220-8235; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

2. Об обязательном экземпляре документов: федер. закон от 29 дек. 1994 г. № 77-ФЗ: ред. от 3 июля 2016 г. // Собр. законодательства Рос. Федерации. 1995. № 1. Ст. 1; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

3. Об оперативно-розыскной деятельности: федер. закон от 12 авг. 1995 г. № 144-ФЗ: ред. от 2 авг. 2019 г. // Собр. законодательства Рос. Федерации. 1995. № 33. Ст. 3349; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

4. О почтовой связи: федер. закон от 17 июля 1999 г. № 176-ФЗ: ред. от 29 июня 2018 г. // Собр. законодательства Рос. Федерации. 1999. № 29. Ст. 3697; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

5. О валютном регулировании и валютном контроле: федер. закон от 10 дек. 2003 г. № 173-ФЗ: ред. от 2 авг. 2019 г. // Собр. законодательства Рос. Федерации. 2003. № 50. Ст. 4859; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

6. Об архивном деле в Российской Федерации: федер. закон от 22 окт. 2004 г. № 125-ФЗ: ред. от 28 дек. 2017 г. // Собр. законодательства Рос. Федерации. 2004. № 43. Ст. 4169; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

7. О персональных данных: федер. закон от 27 июля 2006 г. № 152-ФЗ: ред. от 31 дек. 2017 г. // Собр. законодательства Рос. Федерации. 2006. № 31 (ч. I). Ст. 3451; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

8. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // Собр. законодательства Рос. Федерации. 2006. № 31. Ст. 3448.

9. О ратификации Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: федер. закон от 1 окт. 2008 г. № 164-ФЗ // Собр. законодательства Рос. Федерации. 2008. № 40. Ст. 4499.

10. Об организации предоставления государственных и муниципальных услуг: федер. закон от 27 июля 2010 г. № 210-ФЗ // Собр. законодательства Рос. Федерации. 2010. № 31. Ст. 4179.

11. Об электронной подписи: федер. закон от 6 апр. 2011 г. № 63-ФЗ: ред. от 23 июня 2016 г. // Собр. законодательства Рос. Федерации. 2011. № 15. Ст. 2036; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

12. О лицензировании отдельных видов деятельности: федер. закон от 4 мая 2011 г. № 99-ФЗ: ред. от 2 авг. 2019 г. // Собр. законодательства Рос. Федерации. 2011. № 19. Ст. 2716; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

13. Об утверждении перечня сведений конфиденциального характера: указ Президента Российской Федерации от 6 марта 1997 г. № 188: ред. от 13 июля 2015 г. // Собр. законодательства Рос. Федерации. 1997. № 10. Ст. 1127; 2015. № 29 (ч. II). Ст. 4473.

14. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Российской Федерации от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50. Ст. 7074.

15. Об утверждении Соглашения о свободном доступе и порядке обмена открытой научно-технической информацией государств – участников СНГ: постановление Правительства Российской Федерации от 26 окт. 1999 г. № 1196 // Собр. законодательства Рос. Федерации. 1999. № 44. Ст. 5324.

16. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных: постановление Правительства Российской Федерации от 17 нояб. 2007 г. № 781 // Собр. законодательства Рос. Федерации. 2007. № 48 (ч. II). Ст. 6001. (Утратило силу).

17. Об утверждении Правил делопроизводства в федеральных органах исполнительной власти: постановление Правительства Российской Федерации от 15 июня 2009 г. № 477: ред. от 26 апр. 2016 г. // Собр. законодательства Рос. Федерации. 2009. № 25. Ст. 3060; 2016. № 18. Ст. 2641.

18. Об утверждении Положения о системе межведомственного электронного документооборота: постановление Правительства Российской Федерации от 22 сент. 2009 г. № 754: ред. от 16 марта 2019 г. // Собр. законодательства Рос. Федерации. 2009. № 39. Ст. 4614; Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

19. О лицензировании деятельности по технической защите конфиденциальной информации: постановление Правительства Российской Федерации от 3 февр. 2012 г. № 79 // Собр. законодательства Рос. Федерации. 2012. № 7. Ст. 863.

20. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифро-

вальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя): постановление Правительства Российской Федерации от 16 апр. 2012 г. № 313: ред. от 18 мая 2017 г. // Собр. законодательства Рос. Федерации. 2012. № 17. Ст. 1987; 2017. № 22. Ст. 3154.

21. Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя): постановление Правительства Российской Федерации от 16 апр. 2012 г. № 314 // Собр. законодательства Рос. Федерации. 2012. № 17. Ст. 1988.

22. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства Российской Федерации от 1 нояб. 2012 г. № 1119 // Собр. законодательства Рос. Федерации. 2012. № 45. Ст. 6257.

23. Об утверждении Соглашения о сотрудничестве в формировании информационных ресурсов и систем, реализации межгосударственных программ государств – участников Содружества Независимых Государств в сфере информатизации: постановление Правительства Российской Федерации от 28 мая 2002 г. № 356 // Собр. законодательства Рос. Федерации. 2002. № 23. Ст. 2165.

24. Об электронной цифровой подписи: постановление Межпарламентской Ассамблеи государств – участников СНГ: модельный закон от 9 дек. 2000 г. № 16-10 // Информационный бюллетень. Межпарламентская Ассамблея государств – участников Содружества Независимых Государств. 2001. № 26. С. 310-326.

25. Положение о сертификации средств защиты информации по требованиям безопасности информации: утв. приказом Государственной технической комиссии при Президенте Российской Федерации от 27 окт. 1995 г. № 199. Доступ из справ.-правовой системы «КонсультантПлюс».

26. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18 февр. 2013 г. № 21 // Рос. газ. 2013. 22 мая.

27. Об утверждении Положения о системе сертификации средств защиты информации: приказ ФСТЭК России от 3 апр. 2018 г. № 55 // Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru

28. О порядке присоединения к сетям связи общего пользования и порядке регулирования пропуска трафика сетей связи общего пользования: письмо Минсвязи России от 28 марта 1995 г. № 54-у. Доступ из справ.-правовой системы «КонсультантПлюс».

29. ГОСТ 20886-85. Организация данных в системах обработки данных. Термины и определения (утв. Постановлением Государственного комитета СССР по стандартам от 31 янв. 1985 г. № 240). Доступ из справ.-правовой системы «КонсультантПлюс».

30. ГОСТ 16325-88. Машины вычислительные электронные цифровые общего назначения. Общие технические требования (утв. Постановлением Государственного комитета СССР по стандартам от 9 сент. 1988 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

31. ГОСТ 15971-90. Системы обработки информации. Термины и определения (утв. Постановлением Госстандарта СССР от 26 окт. 1990 г. № 2698). Доступ из справ.-правовой системы «КонсультантПлюс».

32. ГОСТ Р 51170-98. Качество служебной информации. Термины и определения (утв. Постановлением Госстандарта России от 12 мая 1998 г. № 184). Доступ из справ.-правовой системы «КонсультантПлюс».

33. ГОСТ Р 7.0.8-2013. Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения (утв. приказом Росстандарта от 17 окт. 2013 г. № 1185-ст). Доступ из справ.-правовой системы «КонсультантПлюс».

34. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Председателем Государственной технической комиссии при Президенте Российской Федерации 25 нояб. 1994 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

35. Белкин Р.С. Криминалистическая энциклопедия. М.: БЕК, 1997. 342 с.

36. Зинин А.М., Подволоцкий И.Н. Габитоскопия и портретная экспертиза: учебник / под ред. Е.Р. Россинской. М.: Норма: ИНФРА-М, 2016. 160 с.

37. Криминалистический словарь-справочник / авт.-сост. Д.В. Исютин-Федотков. М.: Юрлитинформ, 2010. 464 с.

38. Словарь по криминалистике. 1250 терминов и определений / авт.-сост.: А.М. Багмет [и др.], под ред. А.И. Бастрыкина. М.: ЮНИТИ-ДАНА, 2015. 383 с.

39. Словарь-справочник по оперативно-розыскной деятельности / В.С. Кружилин [и др.]. Воронеж: Воронежский ин-т МВД России, 2014. 44 с.

40. Терминологический словарь-справочник по криминалистике / под общ. ред. В.В. Агафонова. М.: ДГСК МВД России, 2011. 96 с.

41. Юридический словарь для сотрудника ОВД / сост. Т.В. Варлакова [и др.]. Омск: Омская акад. МВД России, 2011. 115 с.

Справочное издание

Составители:
Анисина Светлана Сергеевна
Достов Владислав Владимирович
Усманов Рамиль Ахматович

ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПОДРАЗДЕЛЕНИЙ ОПЕРАТИВНО-РАЗЫСКНОЙ ИНФОРМАЦИИ

Терминологический словарь

Корректура *Е.В. Карнаухова*
Дизайн обложки *Е.К. Булатова*
Тиражирование *А.И. Кубрина*

Подписано в печать 20.12.2019. Формат 60х84/16.
Усл. п. л. 3,5. Уч.-изд. л. 3,0. Заказ № 89.
Тираж 100 экз. Цена свободная.

Научно-исследовательский и редакционно-издательский отдел
Тюменского института повышения квалификации
сотрудников МВД России
625049, г. Тюмень, ул. Амурская, 75.

ISBN 978-5-93160-290-5