МВД России
Санкт-Петербургский университет

Д. И. Якушев

СПЕЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Учебно-методическое пособие

Санкт-Петербург
2024

План-график 2024, поз. 69

УДК 004.9, 351.741
ББК 16
Я49

Якушев Д. И.

Я49 Специальные информационные технологии в правоохранительной деятельности: учебно-методическое пособие / Д. И. Якушев. — Санкт-Петербург: СПбУ МВД России, 2024. — 48 с.

ISBN 978-5-91837-825-0
EDN: RIWEVY

Учебно-методическое пособие подготовлено в соответствии с программой учебной дисциплины «Специальные информационные технологии в правоохранительной деятельности» (разделом 1).

В издании рассмотрены теоретические и практические вопросы использования специальных информационных технологий в правоохранительной деятельности, а также законодательство, регулирующее указанную сферу.

Учебно-методическое пособие предназначено для курсантов, обучающихся по специальности 10.05.05 — «Безопасность информационных технологий в правоохранительной сфере». Некоторые материалы могут быть востребованы слушателями и курсантами других специальностей и направлений при изучении ими основ применения специальных информационных технологий в правоохранительной деятельности, а также преподавателями, адъюнктами, научными и практическими работниками.

УДК 004.9, 351.741
ББК 16

Рецензенты:
Мещерякова Т. В., доктор технических наук, доцент
(Воронежский институт МВД России);
Дунин В. С., кандидат технических наук
(Дальневосточный юридический институт МВД России)

ISBN 978-5-91837-825-0

Оглавление

Список сокращений

АИС	Автоматизированная информационная система
АРМ	Автоматизированное рабочее место
ГИАЦ	Главный информационно-аналитический центр
ЕИТКС	Единая информационно-телекоммуникационная система
ИБД	Информационный банк данных
КУ	Криминалистический учет
ОРИ	Оперативно-розыскная информация
ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦОД	Центр обработки данных
IT	Информационные технологии

Введение

«Кто владеет информацией — тот владеет миром».
Н. Ротшильд

Одной из задач современности является формирование информационного общества — общества, в котором процессы сбора, обработки, анализа, передачи информации, т. е. информационные и коммуникационные технологии, занимают основное место в различных сферах человеческой деятельности.

Стремительное развитие и использование информационных технологий (*IT*) в социально-правовой, культурной, политической, экономической и других сферах общества актуализируют проблему подготовки кадров, способных решать профессиональные задачи в существующем информационно-правовом пространстве. В полной мере сказанное относится и к правоохранительной деятельности, где необходимы специалисты, являющиеся профессионалами в области использования *IT*, применительно к деятельности органов внутренних дел.

Основной целью дисциплины «Специальные информационные технологии в правоохранительной деятельности» является вклад в подготовку специалистов в сфере обеспечения информационной безопасности ОВД и в области компьютерной экспертизы.

В связи с этим основными задачами дисциплины являются:

— подготовка специалистов в сфере обеспечения информационной безопасности и компьютерной экспертизы для ОВД в условиях широкого применения современных *IT*;

— получение слушателями знаний о теоретических, в том числе правовых и организационных основах применения специальных информационных технологий в деятельности ОВД;

— формирование у обучающихся умений и первоначальных навыков применения специальных информационных технологий в деятельности ОВД.

Практически вся деятельность в органах внутренних дел связана с получением и обработкой информации. Под системой информационного обеспечения деятельности ОВД понимается взаимосвязанный комплекс методов, мероприятий и средств, регламентирующий и реализующий процессы создания и функционирования механизма сбора, передачи, переработки, отображения, использования и хранения информации в целях осуществления эффективной деятельности ОВД в сфере охраны общественного порядка, безопасности и борьбы с преступностью. Это отражено и в ст. 11 Федерального закона «О полиции»: «Использование достижений науки и техники, современных технологий и информационных систем», а также в ст. 10 Федерального закона «Об оперативно-розыскной деятельности в Российской Федерации»: «Информационное обеспечение и документирование оперативно-розыскной деятельности».

В рамках настоящего учебно-методического пособия не представилось возможным изложить весь курс дисциплины «Специальные информационные технологии в правоохранительной деятельности». Материал был ограничен

только первым разделом «Специальные информационные технологии в органах внутренних дел», касающимся ведения криминалистических учетов.

До начала изложения материала необходимо определиться с терминологией.

Технология — совокупность оборудования, документации, специалистов и программного обеспечения, предназначенная для достижения желаемого результата.

На западе термин технология часто заменяют англоязычным словосочетанием *Know How*. В качестве примера технологии часто приводят подход к производству автомобилей, предложенный Г. Фордом. До этого сборкой каждого автомобиля занималась своя бригада, осуществляющая весь цикл производства, в которую входили высококвалифицированные рабочие, обладающие всеми необходимыми навыками. Но высокая квалификация подразумевает высокие зарплаты, поэтому цена автомобилей была высока. Для снижения себестоимости Г. Форд:

— Разбил процесс сборки на простые технологические операции, большинство из которых могли выполнять работники низкой квалификации.

— Разработал инструкции для быстрого и качественного выполнения каждой технологической операции.

— Разработал специальные инструменты, увеличивающие скорость и качество работы. Например, ключ для затяжки гаек был снабжен датчиком, измеряющим усилие затяжки, благодаря чему резьба не срывалась, а колеса во время движения не соскакивали.

Примененные нововведения позволили добиться снижения себестоимости продукции и повышения ее доступности для населения.

Технологии разрабатываются применительно не только к технике, но и к другим объектам, например:

— в биотехнологиях объектом приложения являются живые организмы;

— в космических технологиях в качестве объектов может выступать все, что связано с освоением космоса (аппараты, ракеты-носители, живые существа и пр.);

— в *PR*-технологиях (*PR — Public Relations* — связь с общественностью) объектом приложения является общественное мнение;

— в *IT* объектом обработки является информация.

IT является сравнительно новым понятием, которое появилось в связи со значительным возрастанием роли информации и ее объемов. Информация, как и нефть, и руда, является ценным ресурсом.

IT (англ. *Information Technology*) — это технология обработки информации.

Во многих случаях, целесообразно разделять понятия данные и информация. Данные — это копия части окружающего мира, а информация — это результат обработки данных, который может быть осознан. Этот подход не противоречит определению, данному в Федеральном законе «Об информации, информационных технологиях и о защите информации»: «Информация — это сведения независимо от формы их представления». Сведения — от слова ведать, знать, то есть то, что уже дошло, или может дойти до сознания.

Этот подход оправдан и в военной области:

«Информация разведывательная — есть осмысленные сведения, основанные на собранных, оцененных и истолкованных фактах, изложенных таким образом, что ясно видно их значение для решения какой-либо конкретной задачи текущей политики»[1].

Основная задача *IT* — получение необходимой пользователю информации в результате обработки данных. Обработка данных с целью получения информации может производиться и вручную, например, ведение картотеки. Однако в настоящее время это уже редко используется, поэтому, разговор об *IT*, подразумевает автоматизированную обработку на основе современных компьютеров, функционирующих на основе двоичной системы счисления. И, хотя общепринятого определения компьютерной информации на сегодняшний день нет, из сказанного вытекает, что компьютерная информация — это данные, хранящиеся в двоичном коде.

На взгляд автора, вместо используемых сегодня многочисленных названий подобных систем: база данных, банк данных, информационная система и так далее, допустимо использовать один термин — автоматизированная информационная система (АИС). При этом термин автоматизированная информационно-поисковая система (АИПС) представляется некорректным, поскольку поисковая функция в АИС подразумевается изначально, и нет смысла добавлять ее в аббревиатуру. Поэтому в дальнейшем изложении будет использоваться только термин АИС, если иное не предусмотрено в нормативных правовых актах.

Специальные информационные технологии — это *IT*, сфера действия которых ограничена специальной, отличной от обыденной жизни областью. Специальные информационные технологии в правоохранительной деятельности — это *IT*, применяемые в правоохранительной деятельности. Безусловно, это часть жизни общества, однако, несущая в себе специфичные черты, в числе которых и ограничения конституционных прав граждан. Это вовсе не означает, что правоохранительная деятельность нарушает эти права. Она, как и другие сферы жизни общества, существует в рамках действующей Конституции Российской Федерации. Однако некоторые стороны этой деятельности как раз и связаны с теми ограничениями прав и свобод граждан, которые провозглашены Конституцией Российской Федерации. Эти ограничения прав и свобод, с одной стороны, призваны обеспечить жизнеспособность всей правовой системы государства (поэтому деятельность, их реализующая и называется правоохранительной), а, с другой стороны, методы и средства, используемые для осуществления этой деятельности, во-первых, относятся к исключениям, оговоренным в Конституции Российской Федерации, а, во-вторых, методы и средства для их

[1] Плэтт В. Информационная работа стратегической разведки. Основные принципы. — Москва: Иностранная литература, 1958. — 341 с.
Плэтт Вашингтон (1890–1965) — бригадный генерал армии США, один из основоположников стратегической разведки США.

успешной реализации не являются общедоступными, поскольку относятся к государственной тайне.

Во многом, деятельность правоохранительных органов по получению, обработке и использованию специальной информации регламентирована Федеральным законом «Об оперативно-розыскной деятельности в Российской Федерации». Именно поэтому специальная информация, работа с которой является основой ОРД, называется оперативно-розыскной информацией (ОРИ).

Существует несколько определений ОРИ. Однако страницы текста, содержащего теоретические воззрения различных исследователей, хороши для книг, научных изысканий, но не для запоминания, а, тем более, не для понимания. Поэтому далее под ОРИ будет пониматься информация, сопутствующая оперативно-розыскной деятельности (ОРД).

Широкое использование современных *IT* позволяет не только обеспечивать стандартизацию и удобство исполнения документов, но и использовать основные преимущества *IT* — скорость поиска, обработки и передачи двоичной информации, а также значительно увеличить объемы ее хранения.

Здесь, однако, ни в коем случае нельзя впадать в заблуждение, приводящее к отказу от методов правоохранительной деятельности, существовавших до широкого внедрения *IT*. Никакая техника не заменит оперативного сотрудника. В качестве аргумента можно привести тот факт, что за 9 месяцев 2020 года количество *IT*-преступлений в Российской Федерации выросло практически вдвое, и при этом 97 % из них в той или иной мере содержали элементы социальной инженерии — одной из составляющих оперативной работы.

Решения по отказу от старых, проверенных временем, методов работы в пользу новых, только что появившихся, принимались неоднократно. Например, Президент США (1933–1945) Ф. Д. Рузвельт назвал разведку «копанием в чужом белье» и высказал мнение, что все задачи разведка должна решать джентельменски, т. е. гласно. Однако после нападения японцев в 7 декабря 1941 г. на базу Перл-Харбор, когда Америка понесла ощутимые потери, он вынужден был изменить свою точку зрения. Другой пример. В связи с появлением нового вида вооружений — ракет, в СССР при Н. С. Хрущеве были свернуты проекты по разработке новых видов вооружений в сферах артиллерии и военно-воздушных сил, однако 60 лет спустя в ходе специальной военной операции Вооруженных сил Российской Федерации очевидна ошибочность этого подхода.

Поэтому на сегодняшний, несмотря на бурный рост *IT*, основным источником получения ОРИ и, тем более, ее оценки, был и остается сотрудник оперативных подразделений.

Глава 1
Правовые основы применения и история создания криминалистических учетов

§ 1. Правовые основы применения специальных информационных технологий в деятельности органов внутренних дел

Основа — это то, на чем основывается, базируется все здание, построение, наука и т. д. Здесь уместна аналогия с фундаментом здания, сооружения. Если фундамент имеет существенный изъян, то рано или поздно он разрушится в результате внешних или внутренних воздействий, что приведет к разрушению того, что на нем возведено. То же относится и к основам: это положение применимо и к аксиоматике различных наук, и к правовым основам существования государств.

Правовая основа — это система обязательных правовых норм, установленных государством.

Информационное обеспечение ОРД регулируется:

— Конституцией Российской Федерации;

— ст. 11 Федерального закона «О полиции»;

— п. 1 ст. 10 Федерального закона «Об оперативно-розыскной деятельности в Российской Федерации»;

— приказом МВД России «Об утверждении Типового положения об информационном центре МВД, ГУВД, УВД субъекта Российской Федерации, УВДТ, ГУВД-РО СОБ МВД России»;

— приказом МВД России, МЧС России, Министра обороны Российской Федерации, Минфина России, Минюста России, Минтранса России, СВР России, ФСБ России, ФСО России, Росгвардии, ГУСП, Генеральной прокуратуры Российской Федерации, СК России «О порядке формирования направляемой в органы внутренних дел дактилоскопической информации» и др.

В ст. 23 Конституции Российской Федерации закрепляется право граждан на неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. Не допускается распространение информации о частной жизни лица (равно как и сбор, хранение, использование сведений) без его согласия (п. 1 ст. 24), жилище неприкосновенно (ст. 25). Однако ст. 55 Конституции Российской Федерации предусматривает ограничение прав и свобод человека и гражданина федеральным законом, но только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Следовательно, применение правоохранительными органами специальных информационных технологий возможно не только для получения в рамках закона необходимой информации, но и защиты на законных основаниях информационных и имущественных прав и свобод граждан. В ст. 138 Уголовного Кодекса Рос-

сийской Федерации устанавливается ответственность за «нарушение тайны переписки, телефонных переговоров, почтовых и иных сообщений». При этом объективная сторона преступления выражается как в незаконном ознакомлении с содержанием телефонных переговоров и почтово-телеграфной корреспонденции, так и в придании огласке сообщенных гражданами друг другу сведений.

В соответствии со ст. 11 Федерального закона «О полиции» полиция в своей деятельности «обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру».

Полиции предписано применять электронные формы приема и регистрации документов, уведомления о ходе предоставления государственных услуг, взаимодействия с другими правоохранительными органами, государственными и муниципальными органами, общественными объединениями и организациями. Полиция использует специальные информационные технологии, включая средства аудио-, фото- и видеофиксации, при документировании обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий, в том числе в общественных местах, а также для фиксирования действий сотрудников полиции, выполняющих возложенные на них обязанности.

В п. 4 ст. 11 Федерального закона «О полиции» указано, что федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность использования сети «Интернет» и АИС. Согласно п. 18 ст. 12 Федерального закона «О полиции» полиция обязана проводить экспертизу по уголовным делам, при этом также с использованием технических средств.

В соответствии с п. 33 ст. 13 указанного закона полиция имеет право использовать в деятельности информационные системы, видео- и аудиотехнику, кино- и фотоаппаратуру, а также другие технические и специальные средства, не причиняющие вреда жизни и здоровью граждан, а также окружающей среде; вести видеобанки и видеотеки лиц, проходивших (проходящих) по делам и материалам проверок полиции; формировать, вести и использовать банки данных оперативно-справочной, криминалистической, экспертно-криминалистической, розыскной и иной информации о лицах, предметах и фактах; использовать банки данных других государственных органов и организаций, в том числе персональные данные граждан, если федеральным законом не установлено иное.

Полиция в своей деятельности использует достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру (п. 56 ст. 11 Федерального закона «О полиции»).

Полиция имеет право осуществлять ОРД в соответствии с Федеральным законом «Об оперативно-розыскной деятельности в Российской Федерации», который является базовым актом в вопросах применения специальных технических средств, предназначенных для негласного получения информации. Согласно ст. 6 оперативным аппаратам субъектов ОРД в ходе проведения оперативно-розыскных мероприятий разрешается использовать информационные системы, видео- и аудиозапись, кино- и фотосъемку, а также другие технические

и иные средства, не наносящие ущерба жизни и здоровью людей и вреда окружающей среде.

Согласно ст. 6 Федерального закона «Об оперативно-розыскной деятельности в Российской Федерации» для решения задач ОРД позволяется использовать помощь специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе.

Федеральным законом от 7 июля 2003 г. № 126-ФЗ «О связи» установлена правовая основа деятельности в области связи, определены полномочия органов государственной власти по регулированию указанной деятельности, а также права и обязанности физических и юридических лиц, участвующих в указанной деятельности или пользующихся услугами связи. В Законе определены основные положения о связи в Российской Федерации. Статья 16 Федерального закона «О связи» посвящена сетям связи специального назначения, которые предназначены для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка. Порядок подготовки и использования ресурсов единой сети электросвязи Российской Федерации в целях обеспечения функционирования сетей связи специального назначения определен «Правилами подготовки и использования ресурсов единой сети электросвязи Российской Федерации в целях обеспечения функционирования сетей связи специального назначения», утвержденными постановлением Правительства Российской Федерации «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации в целях обеспечения функционирования сетей связи специального назначения».

В отдельную группу таких документов входят ведомственные нормативные акты по вопросам технической политики ОВД, акты, утверждающие перечень новых образцов специальных технических средств, принятых на их вооружение, а также нормативные документы, регламентирующие нормы табельной положенности технических средств, сроки их эксплуатации.

Специфика деятельности ОВД подразумевает накопление больших объемов как открытой, так и конфиденциальной информации, необходимой для осуществления правоохранительной деятельности. Это возможно реализовать только на основе современных *IT*.

Эффективность борьбы с преступностью во многом зависит от правильной организации сбора, концентрации и хранения данных, способных своевременно обеспечить оперативные подразделения и службы ОВД достоверной, полной и точной информацией. Такую информацию, специальным образом систематизированную и размещенную в соответствующих делах или АИС, принято называть учетами.

Значительное место в работе всех правоохранительных органов занимает использование криминалистических учетов, позволяющих принимать обоснованные тактические и процессуальные решения.

Криминалистический учет (далее — КУ) — это система регистрации и хранения информации о лицах, совершивших преступления, о самих преступлениях и связанных с ними фактах и предметах. Он занимает основное место в информа-

ционном обеспечении правоохранительных органов. Совокупный объем учетов органов МВД России охватывает около 95 % криминальных проявлений.

Правовой основой использования КУ в ОРД служат статьи 23, 24, 55 Конституции Российской Федерации, ст. 10 Федерального закона «Об оперативно-розыскной деятельности»; ч. 4 ст. 11, п. 33 ч. 1 ст. 13, ст. 17 Федерального закона «О полиции». Кроме того, эта основа включает Федеральные законы «Об информации, информационных технологиях и о защите информации», а также другие нормативные правовые акты Российской Федерации.

Структура и порядок формирования КУ МВД России определяются ведомственными нормативными актами. Они также используются другими ведомствами, подписавшими приказ «О порядке формирования направляемой в органы внутренних дел дактилоскопической информации», судами Российской Федерации всех уровней судебной системы и соответствующими органами государств — участников стран Содружества независимых государств. Кроме того, существуют нормативные акты по отдельным видам учетов.

К настоящему времени создано единое информационное пространство ОВД России.

Формирование современного массива дактилоскопической идентификации начало осуществляться с принятием Федерального закона «О государственной дактилоскопической регистрации в Российской Федерации».

В настоящий момент формирование дактилоскопических информационных ресурсов осуществляется на основании совместного Приказа МВД России № 659, МЧС России № 717, МО России № 473, Минфина России № 208н, МЮ России № 209, Минтранса России № 385, СВР России № 63, ФСБ России № 429, ФСО России № 376, ФСВНГ России № 145, ГУСПП России № 299, ГП России, СК России от 23.09.2020 «Об утверждении Порядка формирования направляемой в органы внутренних дел дактилоскопической информации».

Вопросы для самоконтроля:

1. Что такое правовая основа?
2. Назовите статью Федерального закона от 7 февраля 2011 г. № 3-ФЗ «О полиции», обязывающую сотрудников использовать в своей деятельности достижения науки и техники.
3. Какая статья Конституции РФ закрепляет право граждан на неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений?
4. Какая статья Конституции РФ предусматривает ограничение прав и свобод человека и гражданина федеральным законом, но только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства?
5. В каком нормативном правовом акте определены структура и порядок формирования оперативно-справочных, розыскных и криминалистических учетов ОВД?

6. Какими законодательными актами регулируется информационное обеспечение ОРД?

7. Предусматривает ли законодатель допуск других ведомств к информации КУ МВД России?

8. Дайте определение криминалистическому учету.

9. Какое понимание может вкладываться в понятие «криминальный учет»?

10. Какими нормативными правовыми актами определяются структура и порядок формирования КУ МВД России?

§ 2. История создания криминалистических учетов

Создание и ведение криминалистических учетов не является изобретением современной информационной эпохи. Одним из первых учетов преступников который известен истории, является список взяткополучателей, обнаруженный голландскими археологами в Сирии близ Бакки, недалеко от Дамаска. Во время раскопок в развалинах здания, ранее используемого в качестве государственного учреждения, был обнаружен полный перечень лиц, занимающих высокие должности, получающих взятки, который датирован около 1400 лет до н. э.

«Практика регистрации и визуальной идентификации лиц, совершивших преступления, существует много столетий. В Древнем Египте для этих целей у человека выбивали передний зуб, в античных Греции и Риме — раскаленным железом на плече выжигали буквенное клеймо. В средневековой Европе лицам, совершившим кражу, как правило, отрезали уши; осужденным за разбойные нападения отсекали нос; нарушившим клятву — палец, а в некоторых случаях и руку; мошенникам на ушах делали надрезы. Законодательство Византийской империи также предусматривало регистрацию преступников путем членовредительства, что нашло отражение в договоре с князем Игорем 945 г.»[1]. За кражу имущества, стоимостью более половины гривны предусматривалось наказание розгами и клеймение (договор Новгорода с Готландом 1270 г.). Уставная грамота великого князя Василия, сына Дмитрия Донского, выданная жителям Двинской земли прямо указывала «татя всякого пятнати». По свидетельству английского купца Р. Ченлора (бывшего в России в 1553–1554 гг. и прибывшего в Москву из Архангельска), за повторную кражу преступнику отрезали часть носа, на лоб ставили клеймо и заключали в тюрьму. Уставная книга Разбойного приказа, действовавшая на Руси в период принятия Судебника 1589 г. и до Уложения 1649 г., также предусматривала членовредительство как меру наказания и акт регистрации преступника. Так ст. 38 содержала санкцию «отсечение руки» за укрывательство особо тяжких преступлений и за кражу, совершенную повторно. В Уложении 1649 г., которое действовало вплоть до Уголовного Уложения 1845 г. также предусматривалось членовредительство. И. Т. Посошков (1652–1726) в «Книге о скудности и богатстве» обосновывал необходимость клеймения в качестве средства предупреждающего совершение повторных преступлений. Ука-

[1] Белов О. А. Криминалистическая регистрация: история, современное состояние и перспективы развития: учебное пособие. — Москва: Юрлитинформ, 2010. — 144 с.

зы Петра I предусматривали, что лица, осужденные к смертной казни, которая заменялась им ссылкой, должны быть заклеймены буквой «В» – вор. Чтобы знак был хорошо различим, и его нельзя было уничтожить, клеймо «многожды накрепко» натирали порохом. Осужденных же к пожизненной каторге в Сибири клеймили буквами «КАТ» — каторга. Во Франции клеймо из букв «*TF*» означало «*Travaux forces*» — принудительные работы; осужденный отбывать наказание гребцом на галеру имел отметку «*GAL*» либо «*G*»; осужденный за кражу — «*U*», а за повторную кражу клеймился второй раз. В Австрии в XVIII в. клеймо указывало не только вид преступления, но и место, где преступление было совершено. Окончательно клеймение во Франции было отменено в 1832 г., а в России — указом «О некоторых изменениях в существующей ныне системе наказаний уголовных и исправительных» от 17 апреля 1863 г. Таким образом, вплоть до середины XIX в. в большинстве случаев для регистрации считалась достаточной визуальная идентификация преступников с помощью клеймления. Скорее всего, это объясняется, во-первых, достаточностью этого подхода в большинстве случаев, а, во-вторых, дороговизной других подходов.

В XVIII–XIX вв. в Германии между городами уже практиковался обмен списками лиц, совершивших мошеннические действия, в которых помимо анкетных данных имелись и описания внешности этих лиц. В начале XIX в. в российской полиции также начинает практиковаться описание внешности человека. Учету с помощью описания подвергались осужденные, подозреваемые в совершении преступлений, а также разыскиваемые лица. Централизованный учет по признакам внешности в полиции отсутствовал. Более успешно действовал данный способ учета в жандармском корпусе, документы которого носили оперативный характер и аккумулировались в «делах-формулярах». Сведения о лицах, поставленных на учет, с 1826 г. концентрировались в штабе корпуса жандармов в алфавитных картотеках. В Санкт-Петербургском архиве на Набережной р. Мойки, д. 16 действовал еще и «Личный алфавит». К 1850 г. архив жандармерии насчитывал до 30 000 «дел-формуляров».

Использование фотографии, изобретенной в 1839 г., с целью запечатления внешности преступника, возможно, начинается ранее 1841 г. В одной из газет, издаваемых в Калифорнии, в ноябре 1841 г. сообщалось, что французская полиция производит фотосъемку лиц, совершивших преступление. К 1870-м гг. во Франции таких фотоснимков насчитывалось до 80-ти тысяч. В Бельгии удалось обнаружить в архиве фотоснимки лиц, отбывавших наказание с 1843–1844 гг. Межгосударственный обмен фото преступников практиковался, по крайней мере, с 1850-х гг.

В России с конца 1850-х гг. в III отделении начали использовать фотографирование лиц, представлявших оперативный интерес. В 1862 г. в Санкт-Петербургской полиции было открыто специальное фотографическое бюро, а с 1867 г. подобная лаборатория начала действовать и в Москве. В 1872 г. было предложено фотографировать преступников в фас и правый профиль. С 1891 г. в Пруссии вводится обязательное фотографирование неопознанных трупов.

С середины XIX в. в Европе учет преступников производился уже с помощью фотоснимков и регистрационных карточек, в которых произвольно

фиксировались некоторые элементы внешности, анкетные данные и способ совершения преступления. Увеличение количества карточек потребовало создания системы, обеспечивающей быстрый поиск в массиве по поступившему запросу. В 1879 г. таким средством стал антропометрический метод регистрации, предложенный А. Бертильоном.

В России система А. Бертильона стала использоваться с 1890 г., когда при сыскном отделении полиции было создано антропологическое бюро, получившее название регистрационной станции. Постановке на регистрационный учет подлежали лица, попавшие в поле зрения сотрудников сыскных подразделений. В 1892 г. в местах, где размещались лица, осужденные к ссылке и ссыльные каторжане, а также в ряде крупных городов, были открыты еще 10 регистрационных станций. С 1890 по 1915 г. сотрудники Санкт-Петербургской регистрационной станции поставили на учет 111 370 человек и установили личность 1538 человек. К 1909 г. антропометрические станции были созданы уже в 89 сыскных отделениях полиции.

Большой резонанс в России вызвал факт установления личности по системе бертильонажа, который имел место 1909 г. В 1902 г. в Москве за убийство матери и двух сестер к 12 годам каторжных работ был осужден А. Кара. После ареста в 1901 г. он был поставлен на регистрационный учет. В январе 1905 г. осужденный А. Кара совершил побег, а в 1908 г. был задержан в Саратове. Сравнив учетные антропометрические данные с результатами измерений, сделанных в 1901 г., специалисты пришли к выводу, что под вымышленной фамилией скрывается осужденный А. Кара. Это было подтверждено и сопоставлением фотоснимков.

Неизменяемость папиллярных линий, точнее, их особенностей, составляющих узор на ногтевых фалангах пальцев рук, их постоянное строение, а также наличие индивидуальной совокупности признаков, позволяют идентифицировать человека (труп). Первая научная классификация папиллярных линий на ногтевых фалангах пальцев рук относится к 1823 г. Современная классификация Ф. Гальтона относится к 1891 г. Таким образом, дактилоскопия развивалась параллельно с бертильонажем и конкурировала с ним некоторое время. Представляется, что отказ от бертильонажа в пользу дактилоскопической регистрации был вызван простотой и большей надежностью последней.

Криминогенная обстановка в России практически не отличалась от европейской. Необходимость регистрации преступников и ведения оперативных учетов диктовало время. «Сведения, полученные от агентов, заносились в особую тетрадь, которая содержала и алфавитный указатель упомянутых имен и псевдонимов. Алфавитные указатели, содержавшие ссылки на конкретные страницы донесений, анализировались отдельно, что позволяло не пропустить имеющуюся информацию о конкретном лице, полученную от разных агентов, а также оценивать источник информации. Принятый подход также позволял быстро найти информацию о членах одной организации.

К 1902 г. Особый отдел располагал именной картотекой, включавшей 65 000 учетных карточек и до 200 000 фотографий государственных преступников и политические алфавитные списки лиц, разыскиваемых полицией с при-

ложением фотографии и состоявших под негласным надзором, а также фамилии тех, кто подлежал задержанию в случае попытки проникнуть в Россию, рассылался всем жандармским губернским управлениям еще со времен Третьего отделения. С лета 1871 г., согласно секретному циркуляру, создавался «Алфавит лиц, политически неблагонадежных» и альбомы с их фотографиями, куда вносились все лица, которые почему-либо обращают на себя внимание правительства, преимущественно в отношении политической неблагонадежности… Вместе с донесением о побеге какого-либо лица (предписывалось) немедленно сообщать подробное описание его примет и, если возможно, доставлять и по 5 фотографий каждого государственного преступника».

16 декабря 1906 г. Министерством юстиции утверждаются «Правила о производстве и регистрации дактилоскопических снимков», а Главное тюремное управление подготавливает циркуляр «О введении дактилоскопии в тюремном ведомстве для регистрации преступников». Процесс дактилоскопирования осуществлялся в присутствии начальника места заключения, который удостоверял своей подписью составленный документ.

К 1917 г. объем массива дактокарт превысил 90 000. В 1907–1916 гг. по дактокартам была установлена личность 1 147 человек.

В 1907 г. при Департаменте полиции был создан Регистрационный отдел с Центральным справочным аппаратом, в который поступило около 1.5 млн именных карточек, ранее рассредоточенных в 19 тематических картотеках. Систематизация картотек путем изъятия дублирующей информации привела к сокращению массива до 0.8 млн. После этого ответы на запросы по существующим учетам производились в течение 3–4 минут. Ежегодно поступало до 150 000 карточек, но на учет ставились только те лица, сведений о которых не имелось в картотеке. Тщательная структуризация информации в начале XX в. позволяла работать с картотекой в несколько миллионов карточек.

«В конце XIX — начале XX в. начали создавать специальные коллекции — новый вид учета. Одна из первых подобных коллекций состояла из фотографических копий всех рукописных текстов, исследованных Е. Ф. Буринским в судебно-фотографической лаборатории при Санкт-Петербургском окружном суде, что позволило разработать общие рекомендации по методике экспертного исследования рукописных текстов. Вероятно, существовала и коллекция, содержащая образцы различных способов технической подделки документов.

Руководство Департамента полиции МВД учредило специальные курсы для будущих офицеров жандармерии, на которых, в частности, читался и курс регистрации преступников»[1]. Осенью 1908 г. по распоряжению министра внутренних дел П. А. Столыпина в Санкт-Петербурге были организованы подготовительные курсы для начальников новых 89 сыскных отделений полиции, на которых предусматривалось и изучение методов уголовной регистрации.

[1] Корниенко Н. А. Российские и международные криминалистические учеты. — Москва: Юридический центр, 2004. — 337 с.

23 сентября 1918 г. нарком Г. Петровский утвердил «Положение о Статистическом отделе Комиссариата внутренних дел», в котором действовали Регистрационные бюро, ведущие учет лиц, совершивших преступления и осужденных. В 1921 г. Регистрационно-дактилоскопическое бюро состояло из 8 сотрудников. 18 февраля 1941 г. приказом № 00232 НКВД СССР был организован Первый специальный отдел, перед которым, в частности, ставились задачи по функционированию алфавитного и дактилоскопического учетов. Система Первых специальных отделов существовала до 1970 года, когда была реорганизована в Главный информационный центр при МВД СССР, который в результате неоднократных переименований в эпоху перестройки с 2004 года стал называться Главный информационно-аналитический центр (ГИАЦ) МВД России. Так эта структура называется и сегодня.

Вопросы для самоконтроля:

1. Дайте определение КУ.
2. Какова датировка известного Вам первого КУ?
3. Как Вы понимаете выражение: «Практика регистрации и визуальной идентификации лиц, совершивших преступления»?
4. Что такое клеймение?
5. Какие методы, применяемые для визуальной идентификации лиц, Вы знаете?
6. Что такое бертильонаж?
7. Когда была разработана технология фотографии?
8. Что представляли собой КУ в начале XX в.?
9. Сколько объектов стояло на КУ в начале XX в.?
10. Оцените время поиска по имевшейся картотеке.

§ 3. Автоматизация криминалистических учетов

До 1960-х гг. наиболее емкими носителями ОРИ были дела оперативного учета. Но этот вид организации хранения ОРИ был пригоден лишь для небольших массивов информации. Как только количество дел начинало исчисляться сотнями, поиск, осуществляемый с помощью перелистывания всех дел вручную, становился физически невозможен. Единственным выходом из создавшегося положения была систематизация информации, содержащейся в делах оперативного учета, которая заключалась в выделении характеризующих ее признаков. Признак — это особенность отличающая рассматриваемый объект от других. Сегодня этот процесс называется индексированием, поскольку сходен с индексами поисковых систем интернета.

На первом этапе должен быть разработан единый понятийный аппарат, который, конечно, не является догмой, но практика показала, что введение новых групп поисковых признаков незначительно повышает релевантность[1] поиска. Оказалось, что дробление признаков в существующих группах оказывает негативное влияние на полноту поиска — слишком детальное описание повы-

[1] Релевантность — соответствие результатов ожиданиям.

шает вероятность ошибки первого рода — пропуска искомого документа. Безальтернативное решение этой задачи, по-видимому, невозможно. Например, поисковые системы Яндекс и *Google* решают эту задачу по-разному, но ни одна из них не достигла идеала.

По результатам тестирования наиболее высокую релевантность показали поисковые запросы, содержащие несколько достоверных фактов, среди которых желательно присутствие редких. Это соотносится с теорией идентификации: чем реже частота встречаемости признака, тем больше его идентификационная значимость. Напомним, что идентификационная значимость признака — это десятичный логарифм от вероятности его проявления (частоты встречаемости), взятый с обратным знаком. Например, если признак встречается только у 10 % людей, то вероятность его появления (p) равна 0.1, а идентификационная значимость (α):

$$\alpha = -\lg(p) = -\lg(0.1) = -(-1) = 1$$

Заметим, что релевантность поиска зависит и от достоверности фактов, как хранящихся в АИС, так и включенных в запрос. У очевидцев событий, восприятие действительности сугубо индивидуально и зависит от множества факторов как внешних, так и внутренних. Для уяснения сказанного рекомендуется просмотр научно-популярного фильма «Теория правды. Честность — основной элемент». Поэтому полезно, наряду с занесенной в АИС информацией, сохранять и оценку достоверности этой информации, носящую качественный характер (например, при поиске лица по АИС информация о нем была пропущена, поскольку по показаниям очевидцев поиск осуществлялся, в числе прочего, по признаку возраста 17–20 лет, а ему было 16 лет).

К 1974 г. насчитывалось до 70 алфавитных картотек, как предусмотренных, так и не предусмотренных нормативными актами МВД СССР. Количество информации, которая требовала анализа неуклонно росло. Поэтому в СССР было начато осуществление перехода от алфавитных картотек к АИС. Этот процесс происходил однонаправленно в разных государствах, независимо ни от уровня экономического развития, ни от географического положения, ни от национального состава, ни от общественного строя.

Переход от алфавитных картотек к АИС позволил в разы увеличить количество рассматриваемых признаков. При этом оказался возможным учет частоты ошибок для различных признаков, что позволило вводить поправочные коэффициенты. Также оказалось возможным сохранять информацию, ранее не вписывавшуюся в совокупность используемых признаков.

Кроме очевидных преимуществ подобный подход имел и негативные стороны:

— Формирование перечня признаков может быть осуществлено только на основе итерационного подхода: он будет корректироваться, исходя из практики его применения.

— Проблема возникает, когда поступивший сигнал не содержит признаков из перечня.

— На формулировку признаков влияют как объективные характеристики информации (полнота, достоверность, относимость), так и субъективные качества лица, выделяющего признаки, поскольку процесс не поддается полной автоматизации.

Возможность поиска по большим массивам информации имеет недостатки, выражающиеся в увеличении вероятности ошибки первого рода, т. е. вероятности того, что информация не будет найдена в случае, когда она имеется. Более того, автоматизация процесса выделения поисковых признаков исходной информации усиливает эту вероятность. Н. Винер писал: «...отдайте же человеку — человеческое, а вычислительной машине — машинное. В этом и должна, по-видимому, заключаться разумная линия поведения при организации совместных действий людей и машин».

Компьютер превосходит человека в скорости выполнения операций, в том числе, операций перебора. Однако мозгу человека, во-первых, доступен эвристический (творческий) поиск решения, а, во-вторых, человек может использовать при поиске информацию, не содержащуюся в запросе, который отрабатывает компьютер.

В процессе развития АИС были выработаны следующие принципы их организации:

— Каждый из объектов учета может быть связан с другими объектами.

— Объект может иметь неограниченное количество значений каждого признака, ни одно из которых не является обязательным.

— Признаки могут иметь иерархическую структуру, например, «Учредители» в объекте «Юридическое лицо».

— Признаки могут быть связаны бинарными (двунаправленными) связями, например, купил — продал, что позволяет автоматизировать поиск смысловых связей между объектами учета.

— Реализовано сопоставление вновь вводимой информации с уже имеющейся в АИС.

— При кодировке запроса условия могут налагаться как на признаки, так и на их связи.

— Запрос формируется из признаков, к каждому из которых может прилагаться набор связей.

— Глубина цепочки связей доходит до 50.

— Описание признака может варьироваться, например, точное, среднее, максимальное, минимальное значение.

— Выдача информации может быть представлена в виде, отличном от стандартного.

— Распределение доступа к информации об объектах и их связях должно варьироваться в зависимости от полномочий сотрудника, инициировавшего запрос.

В качестве основных в СССР существовали две АИС, разработанные во ВНИИ МВД СССР: «Учет» (1966) и «Розыск» (1970). Система «Учет» обеспечивала автоматизированный поиск информации о лицах по неполным совокуп-

ностям признаков. Система «Розыск» — содержала информацию о нераскрытых преступлениях. АИС «Паспорт» (1970-е гг.), содержавшая информацию о пересечении гражданами границы СССР была ликвидирована по указанию высшего руководства страны как «нарушающая права человека».

Экспериментальная эксплуатация (1967–1975 гг.) системы «Учет» позволила оценить приемлемость получаемых результатов для практики и сопоставить несколько вариантов ее реализации. Сначала проверка проводилась в городе с населением 124 000 человек; затем в городе с населением 419 000 человек, и, наконец, в масштабе области с населением 1.338 млн человек, и подтвердила приемлемую работоспособность системы.

В частности, экспериментальная эксплуатация показала практическую нецелесообразность накопления всей имеющейся ОРИ только в централизованных учетах, поскольку количество объектов учета, удовлетворяющих поисковому запросу, значительно возрастает и теряет свою практическую ценность. Отсюда был сделан вывод о необходимости создания структуры АИС на федеральном, региональном и местном уровнях (ИБД-Ф, ИБД-Р и территориальные учеты), пересечение которых возможно лишь для ограниченного контингента.

Кроме того, тестирование системы показало, что более 30 % лиц, взятых на учет, не удовлетворяют назначению АИС, что приводит только к зашумленности выдачи информации на поисковый запрос. Это потребовало, в частности, корректировки раздела признаков «Основания постановки на учет». Оказалась востребованной классификация источников информации на разовые и постоянные.

Экспериментальная эксплуатация системы «Учет» позволила прийти к следующим выводам:

— Информация, заносимая в АИС, должна отвечать целям и задачам ОРД.

— Необходимо предусмотреть возможность внесения изменений в ранее включенную информацию.

— Сбор и фиксацию информации целесообразно производить в территориальных оперативно-розыскных подразделениях.

— Для фиксации исходной информации должны использоваться стандартные бланки, понятийный аппарат и терминология, централизованно разработанные для АИС.

— Поисковые запросы должны составлять оперативные сотрудники со стажем работы на обслуживаемой территории.

— Кодирование информации и запросов к АИС, а также сам поиск должны осуществлять операторы АИС.

— Анализ результатов выдачи информации является компетенцией оперативных сотрудников.

Экспериментальная эксплуатация системы «Розыск» позволила прийти к следующим выводам:

— Низкое качество и несвоевременность информации, предоставляемой оперативными сотрудниками (не отражаются даже обязательные признаки, игнорируется стандартизованное описание примет).

— Отсутствие опыта в составлении запросов.

— Отмечена тенденция к сокращению количества предоставляемой информации.

Кроме того, были сформулированы задачи совершенствования эксплуатации АИС:

— организация контроля за предоставляемой информацией;

— установление режима срочности выдачи информации;

— необходимость проверки поступающей информации по сводкам о совершенных преступлениях;

— необходимость проверки поступающей информации по обеим системам «Учет» и «Розыск»;

— разработка программного обеспечения для автоматизации кодирования запросов;

— регламентация предоставления информации по раскрытым преступлениям;

— обеспечение связи между инициатором запроса и оператором АИС при кодировке запроса.

Учеты ОВД, в которые входят криминалистический, криминологический, оперативный, оперативно-справочный, розыскной, профилактический и административный, являются одним из средств ОРД. Обобщенно их можно назвать криминалистические учеты. Иногда в литературе встречается термин «криминальные учеты». В дальнейшем изложении он использоваться не будет, поскольку словосочетание «криминальный учет» может быть понято как: «незаконный учет криминального происхождения».

Проверка по оперативно-справочным, розыскным и криминалистическим учетам является не только процессуальной обязанностью оперативно-следственных работников всех правоохранительных органов, но и прямо предусматривается рядом ведомственных и межведомственных нормативных актов.

Значение криминалистических учетов заключается в следующем:

1. КУ прочно занимают третье место после личного сыска и оперативной работы. Практически ни одно уголовное дело не расследуется без обращения к КУ.

2. Некоторые деяния, могут быть квалифицированы как преступления только при наличии данных, содержащихся в КУ. Например, подделка или уничтожение идентификационного номера транспортного средства; уничтожение или повреждение памятников истории и культуры; уклонение от уплаты таможенных платежей; невозвращение на территорию Российской Федерации предметов художественного, исторического и археологического достояния и ряд других.

3. КУ являются средством, позволяющим установить неоднократность и рецидив преступлений; совокупность преступлений; судимость и другие.

4. КУ могут использоваться при соединении в одном производстве уголовных дел в отношении нескольких лиц, совершивших несколько преступлений в соучастии.

Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации» возлагает на

МВД России основную нагрузку по организации, ведению и хранению дактилоскопического учета, начавшего действовать с 1 января 1999 г. На законодательном уровне приводится перечень лиц, подлежащих обязательной дактилоскопической регистрации. Определяется сфера использования данных дактилоскопического учета. Дактилоскопический КУ используется для розыска лиц; установления личности; в качестве средства предупреждения и выявления административных правонарушений.

Функционирование коллекций и картотек в экспертно-криминалистических подразделениях МВД России регламентируется «Инструкцией по формированию, ведению и использованию экспертно-криминалистических учетов, картотек, коллекций и справочно-информационных фондов ОВД», утвержденной приказом МВД России от 10 февраля 2006 г. № 70, а также другими ведомственными нормативными актами. Ведение иных КУ и розыскных учетов, введенных по инициативе руководства ОВД, предусмотрено ведомственными подзаконными нормативными актами.

Европейский «Меморандум о взаимопонимании» (1995 г.) предусматривает ведение пяти групп КУ: 1) справочные коллекции; 2) огнестрельное оружие; 3) волокна; 4) исследование документов; 5) лакокрасочные покрытия. В перспективе также предполагалась деятельность групп по исследованию ДНК и обработке изображений.

Деятельность Интерпола направлена на содействие правоохранительным органам государств мирового сообщества в борьбе с преступностью. Одним из направлений этой деятельности является криминалистическая регистрация, т. е. накопление известных фактов и быстрая и корректная выдача информации по запросам. Однако желаемое должно совпадать с возможностями. В начале 1990-х гг. Интерпол столкнулся с проблемой. С одной стороны, количество собранных данных было настолько велико, что превышало возможности их корректной классификации, с другой — значительная часть собранного уже не представляла практической ценности. Например, факт кражи в 1947 г. из Национального музея Австралии коллекции бабочек, или похищение слона из цирка в Швейцарии. «К декабрю 1982 года в Сен-Клу скопилось не менее 3 768 000 карточек на международных уголовников, перечисленных в алфавитном, фонетическом порядке и по способу работы. И при поступлении запроса на информацию все эти дела просматривались вручную». Поэтому даже для фактов о тяжких преступлениях был установлен срок давности в несколько лет, а для менее серьезных — три месяца, после чего информация удалялась. Принятые меры в некоторой степени помогли уменьшить объем хранимой информации, однако в то же время они повысили вероятность безвозвратного удаления информации, которая в будущем могла быть востребована.

Еще одной проблемой является достоверность имеющихся данных, определить которую в некоторых случаях достаточно затруднительно, хотя и необходимо. Это относится не только к данным, поступающим для постановки на КУ, но и к любой оперативной информации, в том числе, рассматриваемой в уголовном процессе.

Для обеспечения конфиденциальности обрабатываемой в Интерполе информации принимались следующие меры. Исходили из положения о том, что, если компьютер имеет доступ к внешнему миру, то и внешний мир имеет доступ к нему самому. Поэтому решили использовать линии связи, выделенные только для нужд полиции. Аналогичная структура информационно-телекоммуникационных сетей связи применена и в ЕИТКС МВД России (см. § 3 главы 2). Она позволяет до минимума снизить вероятность получения несанкционированного доступа к данным со стороны интернета, но риск получения несанкционированного доступа со стороны инсайдеров — сотрудников, допущенных к обработке информации, — все равно остается.

Вопросы для самоконтроля:

1. Что относится к объектам КУ?
2. Какова система организации КУ?
3. Какова структура наиболее релевантных поисковых запросов?
4. Что такое признак?
5. Что такое идентификационная значимость признака?
6. Когда в СССР были разработаны первые АИС?
7. Каковы сроки хранения информации об объекте на КУ?
8. Что такое достоверность данных?
9. Как оценивается достоверность данных?
10. Как обеспечивается конфиденциальность компьютерной информации, составляющей учеты Интерпола?

Глава 2
Автоматизированные информационные системы для ведения криминалистических учетов МВД России

§ 1. Криминалистические учеты как средство информационного обеспечения оперативно-розыскной деятельности

Процесс исторического развития информационного обеспечения правоохранительной деятельности не ставил под сомнение необходимость его осуществления. Однако место и структура информационных подразделений в системе МВД неоднократно менялись.

«Длительные дискуссии о кадровом составе подразделений оперативной информации МВД России определили их вхождение в состав подразделений криминальной милиции»[1]. Подобное решение было обусловлено, во-первых, характером решаемых ими задач, а, во-вторых, тем, что квалифицированная обработка оперативной информации требует навыков оперативной работы. Именно поэтому основу подразделений, осуществляющих информационное обеспечение ОРД должны были составлять высококвалифицированные сотрудники оперативных подразделений. В 2003 г. на базе оперативно-сыскных отделов криминальной милиции были созданы подразделения ОРИ.

Основное содержание ОРИ составляют сведения о лицах и фактах их криминальной активности. Источниками ОРИ могут являться различные объекты:

— данные на учитываемых лиц, организованные в виде алфавитно-справочных картотек;
— словесные портреты;
— списки связей объекта;
— справочные карточки на нераскрытые преступления;
— лица, проходящие по уголовным делам и делам оперативного учета;
— информация в КУ;
— справки о результатах проведения оперативно-розыскных мероприятий;
— дактокарты;
— фотографии;
— видеоматериалы;
— фотокомпозиционные портреты;
— рукописные документы и образцы подписи и др.;

В соответствии с ведомственными нормативными актами к числу источников ОРИ могут быть отнесены сведения, содержащиеся в проверочных материалах, карточках и делах оперативного учета, сообщениях штатных негласных сотрудников, справках и рапортах сотрудников оперативных подразделений,

[1] Указание первого заместителя министра внутренних дел России от 9 января 1996 № 1/264. Нормативно-правовые акты приведены в соответствии с данными официального интернет-портала правовой информации Pravo.gov.ru (дата обращения: 20.02.2024).

а также производные от указанных информационные материалы. Формы и содержание этих документов могут разниться.

Объекты ОРИ можно разделить на три группы: лица, попавшие в поле зрения правоохранительных органов; предметы, связанные с преступной деятельностью; факты, связанные с преступной деятельностью. Для обеспечения поиска по КУ каждая группа разбита на категории.

Р. С. Белкин определил криминалистическую регистрацию как «систему КУ определенных объектов – носителей информации, используемую для раскрытия, расследования и предупреждения преступлений».

Основанием для постановки на КУ являются документы первичного учета — статистические карточки, которые представляются оператору АИС субъектами регистрации. Именно от полноты и достоверности данных, предоставленных для постановки на КУ, зависит впоследствии полнота и достоверность, выдаваемой АИС информации.

Для постановки на КУ каждый объект, будь то лицо или факт, необходимо описать — выделить признаки, которые в своей совокупности будут отличать объект постановки от других. Именно по этим признакам проводится и проверка по КУ — формируется ответ на поступивший запрос. Если совокупности признаков объекта, стоящего на учете и проверяемого совпадают, то говорят об оперативной идентификации, если же имеют место некоторые расхождения, то об оперативном ориентировании. Установление подобных связей и является основным назначением информационного обеспечения ОРД. При составлении запросов на поиск информации в АИС важно пользоваться терминами, установленными нормативными актами МВД России для заполнения информационно-поисковых карточек.

Криминалистические учеты позволяет систематизировать данные, содержащиеся в различных источниках и создать условия для их использования правоохранительными органами независимо от времени и региона. Специфика КУ состоит в конфиденциальном характере содержащейся в нем информации, и, соответственно, ограниченном круге должностных лиц, допущенных к ее использованию.

Криминалистические учеты подразделяются на централизованные оперативно-справочные, криминалистические и розыскные.

Справочный учет содержит информацию, получение которой связано с функционированием различных звеньев системы МВД России, однако ее использование доступно и другим ведомствам. С его помощью решаются задачи ОРД: установление фактов совершения преступлений в прошлом; установление фактов проживания; установление транспортных средств и водителей, а также другие сведения. Изначально, справочное назначение учетов предопределило в качестве их формы алфавитные картотеки, которые впоследствии были преобразованы в АИС.

Оперативно-розыскной учет содержит информацию, применяемую только в рамках ОРД, использующуюся для розыска лиц, скрывающихся от правосудия, установления связей между событиями и конкретными лицами. Заметим,

что в США к ответу на запрос присоединяются сведения о сотрудниках, которые ранее интересовались этим объектом учета. Это дает возможность, с одной стороны, осуществлять взаимодействие между субъектами ОРД по объекту их заинтересованности, а, с другой стороны, способствует обеспечению собственной безопасности.

Криминалистические учеты можно рассматривать в виде системы информации, ее признаков, связей между ними, а также программного, аппаратного и кадрового обеспечения АИС. В настоящее время в рамках ИСОД функционируют более ста различных КУ. Основанием для постановки на учет служат: уголовные дела; розыскные дела; дела по установлению личности и другие источники.

Различают три вида криминалистических учетов:

— Оперативные учеты. Оперативный учет — это массив сведений, собираемых и систематизируемых в АИС в целях обеспечения ОРД.

— Централизованные оперативно-справочные, экспертно-криминалистические, розыскные учеты, криминалистические коллекции и картотеки. Централизованный оперативно-справочный учет характеризуется большим массивом объектов учета при их кратком описании. Основное назначение данного вида учета — проверка установленных сведений об объекте и его местонахождении. Этот КУ ведется в форме пофамильного и дактилоскопического учета. Централизованный розыскной учет содержит значительно больше сведений об объекте учета, выполняя наряду с оперативно-справочной функцией сравнение установочных данных и сходных внешних описаний. Постановке на централизованный розыскной учет подлежат лица, объявленные в федеральный розыск; транспортные средства; утраченное и выявленное оружие и иное вооружение; похищенные и изъятые номерные вещи и документы; похищенные предметы, имеющие культурную ценность. Централизованный криминалистический учет — это массив информации о лицах, предметах (следах) и веществах, обладающих идентификационными признаками. На этот КУ ставятся лица, пропавшие без вести; лица, не способные по состоянию здоровья или возрасту сообщить данные о своей личности, а также неопознанные трупы.

— Криминологические, профилактические, административные учеты. Ведение криминологических учетов направлено на прогнозирование состояния преступности, а также связанных с ней факторов. Объектами профилактических учетов являются лица, склонные к совершению преступлений. Объектами административных учетов являются лица, совершившие административные правонарушения, а также предметы, оборот которых ограничен на территории Российской Федерации.

Каждая разновидность может быть представлена на трех уровнях: федеральном, региональном и территориальном.

1. Территориальные криминалистические учеты ведутся на уровне ОВД аналитической группой или выделенным сотрудником и содержат сведения об объектах, представляющих оперативный интерес на обслуживаемой территории.

2. Криминалистические учеты, ведущиеся на региональном уровне (ИБД-Р), содержат полную информацию по обслуживаемому региону. Поступление информации в ИБД-Р осуществляется путем заполнения исходных документов и представления их в информационном центре УМВД региона, порядок которого определяется нормативными документами МВД России и региона. Общими требованиями к поступающим сведениям являются: достоверность, полнота, качественное оформление, своевременность, актуальность. Предусмотрена коррекция информации, введенной ранее.

Исходными документами, формирующими ИБД-Р являются информационно-поисковые карты (ИПК), идентификационные карты, опознавательные карты, учетные алфавитные карты и обычные карты (например, постановление по федеральному розыску, карты по иностранцам и лицам без гражданства). Указанные формы содержат достаточно полные и, по возможности, формализованные (т. е. упорядоченные и закодированные) признаки объекта в форме, удобной как для ввода в АИС, так и для использования в картотеке.

ИБД-Р разделены на подсистемы:

— АИС учета особо опасных и квалифицированных преступников (АИПС «Досье»), интегрированная с централизованной фотовидеотекой ГИАЦ МВД России.

— АИС учета нераскрытых и раскрытых особо опасных (квалифицированных) насильственных преступлений, если есть основания ожидать повторения их теми же лицами или обученными ими другими правонарушителями (АИПС «Насилие»).

— АИС учета правонарушений и преступлений, совершенных иностранцами и лицами без гражданства, а также в отношении них (АИПС «Криминал-И»).

— АИС учета сведений о хищениях ценностей из металлических хранилищ (АИПС «Сейф»).

— АИС учета пропавших без вести, неопознанных трупов и лиц, не способных по состоянию здоровья или возрасту сообщить данные о своей личности (АИПС «ФР-Опознание»).

— АИС учета лиц, объявленных в федеральный розыск («ФР-Оповещение»).

— АИС учета утраченного или выявленного огнестрельного оружия (АИПС «Оружие-МВД»).

— АИС похищенных номерных вещей (АИС «Вещи»);

— АИС разыскиваемых транспортных средств (АИПС «Автопоиск»).

— АИС «Автомототранспорт» — содержит информацию о транспортных средствах, зарегистрированных на обслуживаемой территории.

— АИС учета похищенных предметов, имеющих культурную ценность (АИПС «Антиквариат»).

— АИС учета похищенных и изъятых номерных вещей, документов, ценных бумаг общегосударственного обращения (АИПС «Вещь»).

— АИС «Досье-Мошенник» — содержит информацию о лицах, совершавших мошеннические преступления.

— АИС «Гастролеры» содержит информацию о лицах, представляющих оперативный интерес для ОВДТ, а также о вещах, похищенных на объектах транспорта.

— АИС «Наркобизнес» содержит информацию по незаконному обороту наркотиков.

— АИС «Спецаппарат» — содержит информацию для работы со спецаппаратом.

— АИПС «Радар» — содержит информацию о лицах, освобождающихся из мест лишения свободы на обслуживаемую территорию.

— АИС «Адмпрактика-У» — содержит информацию о лицах, привлеченных к ответственности за совершение административных правонарушений.

— АИС «Реестр лиц, подвергнутых задержанию».

— АИС «ЕГРЮЛ», «ЕГРИП» — единые государственные реестры юридических лиц и индивидуальных предпринимателей.

Учет ведется УФНС по Санкт-Петербургу и УФНС по Ленинградской области. По запросам может быть выдана справочная информация об организациях, зарегистрированных на территории Санкт-Петербурга и Ленинградской области. Предусмотрено выполнение запросов по юридическому адресу и наименованию организации, а также по установочным данным руководителя. По данному учету подразделения могут самостоятельно просматривать информацию через базу «ИБД-Р».

— АИС «*Notebook*» содержит информацию, извлеченную из записных книжек и других носителей, изъятых сотрудниками ОВД.

— АИС «Невод-Р» — предоставление информации сотрудникам СК России.

— АРМ «Арсенал-93» предназначено для сотрудников следственных подразделений.

— АРМ «ГРОВД» создан с целью информационного обеспечения оперативно-розыскной и управленческой деятельности территориальных подразделений ОВД и др.

Кроме КУ ведутся учеты, отражающие информацию о функционировании МВД России:

— АИС правового информирования ОВД (СТРАС «Юрист»).

— АИС «Кадры» предназначена для повышения уровня информационного обеспечения деятельности кадровых подразделений МВД России.

— АИС штабных подразделений ОВД.

— АИС «Федеральная картотека личного состава ОВД» служит для централизации персонального учета лиц рядового и младшего начальствующего состава МВД России.

— АИС «Ведомственный федеральный банк данных удостоверений МВД России» служит для автоматизации оформления и выдачи служебных удостоверений сотрудникам ОВД. Кроме этого, система предназначена для хранения, учета и обработки сведений о выданных служебных удостоверениях и лицах, на которых они оформлены.

— АИС «Социальная защита» содержит сведения о членах семей сотрудников ОВД России, погибших при исполнении служебных обязанностей, и сотрудниках, ставших инвалидами вследствие военной травмы.

— АИС «Боеготовность» служит для совершенствования информационного обеспечения служебно-боевой подготовки в МВД России. Подсистемами являются АИС «Учет дипломов» и АИС «Профессиональная подготовка».

— АИС «Банк данных отдельных документов кандидатов на службу в МВД России и лиц, уволенных со службы из МВД России» содержит данные о сотрудниках, дискредитировавших себя за период прохождения службы и уволенных по отрицательным мотивам, либо кандидатах на службу, не соответствующих требованиям, установленным ст. 29 Федерального закона «О полиции».

— АИС «Дежурная часть» включает информацию по соответствующим учетам, нормативным и инструктивным документам, а также необходимую справочную информацию.

— АИС «Сводка» предназначена для учета поступающей в ОВД оперативной информации, ее статистической обработки и составления отчетов.

— АИС «Письмо» предназначена для сотрудников секретариатов. Программное обеспечение предусматривает решение двух основных задач: «Письма граждан» и «Особый контроль».

— АИС «Секретарь» решает следующие основные задачи: «Секретариат», «Контроль (секретариат)», «Разносная книга», «Нормативный акт», «Контроль (нормативный акт)», «Коллегия», «Приказ», «Словарь разверсток», ряд из которых имеет свои подзадачи, например, «Исполнение», «Архив» и т. п.

— АИС дистанционного обучения — проведение занятий с личным составом ведущими специалистами департаментов МВД России по направлениям деятельности служб.

На отдельный КУ ставятся лица, оказывающие содействие ОВД в борьбе с преступностью на конфиденциальной основе.

В ИБД-Р реализован поиск информации по любой совокупности объектов и реквизитов.

В экспертно-криминалистических подразделениях регионального уровня ведутся:

— АИС пуль, гильз и патронов со следами оружия (пулегильзотеки);

— АИС поддельных денежных знаков и ценных бумаг;

— АИС поддельных документов, изготовленных полиграфическим способом;

— АИС дактилоскопической информации;

— АИС устной речи;

— иные АИС, например, поддельных медицинских рецептов.

Помимо КУ на региональном уровне создаются коллекции и картотеки.

Во всех региональных информационных центрах обеспечен доступ в федеральную базу Главного информационно-аналитического центра (ГИАЦ) МВД России.

3. Федеральные КУ (ИБД-Ф) ведутся на уровне МВД России в ГИАЦ и ЭКЦ МВД России и называются централизованными. ИБД-Ф на базе ГИАЦ МВД России накапливает информацию, поступающую из ИБД-Р, необходимую для ведения федеральных учетов, с отсылкой за уточнением в конкретный ИБД-Р. Кроме перечисленных выше АИС на уровне ГИАЦ МВД России создан и функционирует АИС оперативно-розыскного назначения – «АБД-Центр».

ГИАЦ МВД России координирует внедрение и развитие АИС общего пользования и оперативно-розыскного характера. Структура и основные задачи ГИАЦ МВД России представлены на сайте МВД России.

В настоящее время в ОВД на всех уровнях управления функционируют более ста различных учетов. В некоторых из них реализована возможность обработки графической информации.

Информация, содержащаяся в АИС, имеет оперативно-розыскное значение только при условии постоянного ее обновления, пополнения, своевременного изъятия устаревших данных, а также корректного поиска по запросам. Работа с документами разделена на два режима: справочный режим и режим работы с первичными документами. Справочный режим предназначен для получения информации без возможности редактирования или удаления. Режим работы с первичными документами предназначен для получения максимально полной информации по объекту и дает возможность редактирования и удаления данных.

В подразделениях транспортной полиции ведутся АИС, имеющие как криминалистический, так и розыскной характер: преступников, совершивших преступления на объектах транспорта, и лиц, подозреваемых в их совершении; нераскрытых преступлений; похищенных вещей и грузов.

Значение КУ состоит не только в возможности обеспечения справочной информацией субъектов правоохранительной деятельности, но и выдаче аналитической информации, полученной на основе накопленных данных.

Между объектами учета могут существовать связи, выявление которых уже при тысячах объектов, вручную не представляется возможным. Существующее программное обеспечение позволяет выявлять эти связи на значительную глубину. Конечный результат при этом во многом зависит от качества и полноты заполнения документов первичного учета.

Существующая организация КУ повышает оперативность и качество принимаемых решений по реализации оперативной информации. Они позволяют осуществлять системный анализ накопленных данных и принятие решений по их реализации.

Важными источниками получения ОРИ являются данные, исходно не относящиеся к оперативной информации, накапливаемые на информационных ресурсах как государственных, так и частных организаций. Доступ к подобной информации возможен, в частности, на основе п. 4 ст. 13 Федерального закона «О полиции»; ст. 6 Федерального закона от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»; постановления Правительства Российской Федерации от 23 сентября 2020 г. № 1526 «О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» инфор-

мации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации».

К подобным ресурсам можно отнести:

— Информационные ресурсы других правоохранительных органов.

— Информационные ресурсы Федеральной таможенной службы Российской Федерации.

— Информационные ресурсы Военных комиссариатов Министерства обороны Российской Федерации.

— Данные аэрофотосъемки и космической разведки, которые могут использоваться, например, для выявления посевов наркосодержащих культур.

— Данные глобальных навигационных спутниковых систем (ГЛОНАСС, *GPS*, *Beidou* и других).

— На информационные ресурсы Федеральной налоговой службы Российской Федерации помимо накопления налоговой информации Федеральным законом «О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации» возложено формирование и ведение единого федерального информационного регистра, содержащего сведения о населении Российской Федерации, который должен начать функционировать с 1 января 2026 года. Регистр будет содержать записи актов гражданского состояния с 1926 года. О каждом гражданине будет информация по 19 пунктам: ФИО, пол, национальность, место жительства, родственные отношения, сведения о рождении и смерти и другие данные.

— Информационные ресурсы государственных служб наблюдения за состоянием природной среды, государственного экологического контроля и других.

— Компании, внесенные в Реестр организаторов распространения информации в сети «Интернет», обязаны хранить информацию пользователей в течение полугода. В частности, это: Яндекс.Почта, Яндекс.Диск, Яндекс.Район, *BlaBlaCar*, 2*GIS*, ВКонтакте, *Telegram*, Авито, *Rutube*, Хабр, *Tinder*, *Snapchat*, Стихи.ру, Проза.ру.

— Согласно «пакету законов Яровой», сотовые операторы обязаны хранить данные соединений в течение полугода.

— АИС медицинских учреждений, некоторые из которых приведены в таблице 1.

Таблица 1

Формы медицинских учетов

Название	Номер формы
Журнал учета приема больных и отказов в госпитализации	001/у
Журнал записи оперативных вмешательств в стационаре	008/у
Протокол (карта) патологоанатомического исследования	013/у
Медицинское заключение по комиссионному освидетельствованию лица, в отношении которого решается вопрос о признании его умалишенным	056/у
Статистическая карта выбывшего из психиатрического (наркологического) стационара	066-1/у-02
Медицинская карта больного, получающего помощь в амбулаторных условиях	025/у
Направление на медико-социальную экспертизу медицинской организацией	088/у
Карта обратившегося за психиатрической (наркологической) помощью	030-1/у-02
Именной список призывников, направленных для систематического лечения	054/у
Книга записи вызовов врача на дом	031/у
Журнал записи амбулаторных операций	069/у
Извещение о больном с впервые в жизни установленным диагнозом наркомании (токсикомании)	091/у
Журнал учета инфекционных заболеваний	060/у
Справка о временной нетрудоспособности в связи с бытовой травмой, операцией аборта	095-1/у
Акт стационарной, амбулаторной, заочной, посмертной судебно-психиатрической экспертизы	100/у
Акт психиатрического освидетельствования осужденного	101/у
Акт психиатрического освидетельствования лица, находящегося на принудительном лечении	104/у

Срок хранения всех перечисленных документов в медицинских учреждениях и их архивах в зависимости от значимости колеблется от 1 года до 50 лет.

Вопросы для самоконтроля:

1. Какие группы информационных ресурсов централизованных учетов Вы знаете?
2. Какие категории граждан являются объектами учета межведомственного дактилоскопического массива личного состава МВД России?
3. Какие учеты относятся к розыскным?
4. Что включается в информационные ресурсы об оружии?
5. Какова структура ГИАЦ МВД России?

6. Каковы основные задачи ГИАЦ МВД России?

7. Назовите известные Вам оперативно-справочные учеты.

8. Перечислите известные Вам учеты иных государственных и негосударственных организаций.

9. Каковы сроки хранения информации на учетах иных организаций?

10. Какую информацию содержат учеты ФНС России?

§ 2. Программное и аппаратное обеспечение, применяемое в автоматизированных информационных системах МВД России

АИС, как и любой объект, подвержена действию времени.

Жизненный цикл АИС – это непрерывный процесс с момента принятия решения о необходимости ее создания до утилизации.

Продолжительность жизненного цикла современных АИС составляет около 10 лет, что превышает сроки морального и физического старения аппаратных и программных средств, используемых при ее реализации. Поэтому, как правило, в течение жизненного цикла системы проводится ее модернизация, после чего все функции системы должны выполняться с не меньшей эффективностью. На практике решение этой задачи наталкивается на многочисленные трудности, например, почти треть проектов АИС оказываются незавершенными, 50 % не завершаются в установленные сроки. Основной причиной подобного положения дел сложность проектов, обусловленная новизной технологий, большим количеством объектов и неочевидностью существующих связей.

Обеспечение качественного технического обслуживания АИС требует привлечения специалистов высокой квалификации, которые в состоянии осуществлять техническое сопровождение и обновление программного обеспечения АИС, настройку и эксплуатацию серверного и коммуникационного оборудования, а также восстанавливать работоспособность системы при сбоях и авариях. Затраты на сопровождение и техническое обслуживание АИС в течение жизненного цикла оцениваются более чем в 70 % ее начальной стоимости. Эти средства выделяются не всегда.

Процесс проектирования АИС регламентирован следующей документацией:

— ГОСТ 34.601—90. Информационная технология. Автоматизированные системы стадии создания.

— ГОСТ Р ИСО/МЭК 12207:2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств».

— Некоторые технологии разработки АИС, например, *Custom Develoment Method* (методология *Oracle*); *Rational Unified Process* — технология итеративной модели разработки; *Extreme Programming* — технология организации взаимодействия между участниками разработки.

Состав современных АИС, как и состав большинства других высокотехнологичных изделий, удобно подразделять на две части: аппаратную (*hardware*) и программную (*software*). Описание структуры жизненного цикла программ-

ной части АИС, достаточно подробно разработано в ГОСТ, и представляет из себя перечисление работ, которые необходимо осуществить при создании, эксплуатации и утилизации АИС. Анализ этого перечня показывает, что процессы жизненного цикла программного обеспечения АИС аналогичны процессам жизненного цикла других изделий и включают в себя:

1. Принятие решения о разработке АИС. На этом этапе обосновывается необходимость создания новой АИС, включающая в себя актуальность и планируемые технико-экономические показатели, а также анализ рынка.

2. Разработка технического задания на АИС. Техническое задание — это документ, определяющий цель создания АИС, а также структуру и конкретные характеристики системы. Допускается, что некоторые из них будут заданы жестко, например, российское программное обеспечение, а для других возможны вариации, например, выбор конкретной системы управления базами данных. Техническое задание — это стратегический документ, который определяет, как направление движения, так и некоторые частные решения в рамках этого направления. И, если направление движения в подавляющем большинстве случаев остается неизменным, то некоторые частные решения могут быть изменены в процессе осуществления разработки, поскольку детальный учет всех нюансов на начальных этапах принципиально невозможен. Чаще всего, изменения в техническое задание на разработку АИС вносятся при совместной работе над документом заказчика и исполнителя. Поиск исполнителя производится путем объявления тендера на разработку. На этом же этапе разрабатывается проект договора на разработку, а также конкретные требования к сопровождающей документации, образцы актов приемки отдельных этапов работ и актов приемосдаточных испытаний.

Заметим, что разработку любых достаточно сложных изделий невозможно осуществить за один шаг, поэтому этот процесс многоступенчатый, состоящий из нескольких этапов, каждый из которых приближает к поставленной цели — разработке АИС с требуемыми характеристиками. Такой подход называют итерационным. Итерация — это совокупность действий, приближающая к решению поставленной задачи. При этом нельзя утверждать, что результаты уже завершенных итераций являются догмой, чем-то неизменным. Вполне может оказаться, что для завершения (или оптимизации) решений, которые требуется достичь на завершающих этапах разработки, необходимо внесение изменений в результаты, полученные на предыдущих этапах. Тогда оказывается необходимым проделать заново некоторую часть ранее завершенной работы.

Отдельно остановимся на вопросе обеспечения информационной безопасности АИС. Актуальность этой составляющей разработки современных АИС, пожалуй, не требует дополнительной аргументации. Треугольник информационной безопасности: конфиденциальность, целостность и доступность, является теоретической основой осуществляемых разработок. Однако для вновь каждой разрабатываемой системы его конфигурация будет иметь свои особенности. При этом практика показывает, что попытки обеспечения информационной безопасности АИС после того, как она уже разработана, не приводят к успеху, то есть не могут обеспечить требуемый уровень защищенности. По-

этому решения, направленные на обеспечение информационной безопасности разрабатываемой АИС должны закладываться, если не на уровне принятия решения о разработке, то, во всяком случае, в техническом задании они должны быть подробно расписаны.

3. Разработка программного обеспечения осуществляется исполнителем в продолжение всего времени работы над проектом. Начало работ, скорее всего, относится еще ко времени, предшествующему подписанию договора с заказчиком, что диктуется как необходимостью уточнения требований заказчика, так и необходимостью уточнения объемов предстоящих работ. Завершение же работ ограничено договором сопровождения разработанного программного обеспечения. Это обусловлено несколькими обстоятельствами. Во-первых, ни одно достаточно сложное программное обеспечение (сюда относится и программное обеспечение всех АИС) не может быть написано с первого раза без ошибок. Ошибки могут выявляться как в процессе разработки исполнителем, так и в процессе промежуточного тестирования по результатам завершения отдельных этапов, так и уже при эксплуатации после передачи разработанной АИС заказчику. Это необходимо учитывать, как при разработке технического задания, так и при разработке договора на сопровождение программного обеспечения после его передачи заказчику.

4. Заказчику необходимо заботится не только о разработке, но и о последующей эксплуатации АИС. Это относится к простоте, удобству и надежности повседневного использования АИС. Помимо обучения пользователей должна быть разработана эксплуатационная документация, позволяющая устранить большинство возникающих проблем без участия представителей разработчика.

5. Не все возникающие с АИС проблемы могут быть устранены на стороне заказчика. Поэтому должно быть предусмотрено как гарантийное, так и послегарантийное обслуживание вводимой в эксплуатацию АИС.

6. Жизненный цикл АИС значительно превышает жизненные циклы как программного, так и аппаратного обеспечения, используемых при реализации АИС. Поэтому при разработке необходимо предусмотреть возможности и пути модернизации для АИС, которые уже эксплуатируются.

Относительные затраты времени на разработку АИС оцениваются как:

— формулировка требований — 10 %;
— определение спецификаций — 10 %;
— проектирование — 15 %;
— кодирование — 20 %;
— автономное тестирование — 25 %;
— тестирование — 20 %.

Далее сформулированы некоторые проблемы внедрения АИС.

1. Функционирование АИС сопровождается множеством форм учетных и отчетных документов, объем которых непрерывно увеличивается, а информация дублируется.

2. Раз в несколько лет появляется новая технологическая платформа (как аппаратура, так и программы), которая во многом не поддерживает предыду-

щие. При этом конвертация данных не всегда возможна или происходит с деформацией данных. При этом жизненный цикл АИС оценивается в 10 лет.

3. Некоторые сотрудники просто не знают о появлении новых АИС.

4. Между разработчиками АИС и непосредственными пользователями должна быть налажена обратная связь.

Одной из необходимых составляющих АИС является программное обеспечение. Для программного обеспечения обработки информации АИС используются системы управления базами данных (СУБД). Критической величиной при этом является количество записей в базе данных. Если их 1 - 2 млн, то хорошо справляются СУБД *MySQL* и *Oracle Database*. Права на оба продукта принадлежат корпорации *Oracle*, США. Если же количество записей превышает 10 млн, то остается только *Oracle*. В частности, при разработке приложений ИБД-Р использовалась СУБД *Oracle*.

Из-за большого количества уязвимостей и *backdoor*[1] в импортном программном обеспечении вышел Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», который гласит, что:

«а) С 31 марта 2022 г. заказчики не могут осуществлять закупки иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации»[2].

«б) С 01 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктуры»[3].

Постановлением Правительства Российской Федерации от 22 августа 2022 г. № 1478 утверждены требования к программному обеспечению на значимых объектах критической информационной инфраструктуры Российской Федерации[4], в которых сказано, что программное обеспечение, используемое органами государственной власти, «должно быть включено в единый реестр российских программ для ЭВМ и баз данных»[5].

---

[1] *Backdoor* (англ. — черный ход) — дефект программного обеспечения, намеренно встраиваемый в него разработчиком, который позволяет получить несанкционированный доступ к данным или удаленному управлению.

[2] Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» / Официальный интернет-портал правовой информации Pravo.gov.ru: сайт. — URL: http://publication.pravo.gov.ru/Document/View/ 0001202203300001 (дата обращения: 15.09.2023).

[3] Там же.

[4] Утверждены требования к программному обеспечению на значимых объектах критической информационной инфраструктуры РФ / Доступ из СПС «КонсультантПлюс»: сайт. — URL: https://www.consultant.ru/law/hotdocs/76883.html?ysclid=lmksitiw6c819732442 (дата обращения: 15.09.2023).

[5] Там же.

Поскольку в корпорации *Oracle* нет (и не предвидится) 50 % российского капитала, то в единый реестр программ для ЭВМ и баз данных СУБД попасть не может. Поэтому на официальном сайте реестра[1] предлагается заменить СУБД *Oracle* на программное обеспечение, присутствующее в реестре. Насколько эта замена окажется приемлемой в эксплуатации — покажет время.

Шаг этот, безусловно, болезненный, дорогостоящий, трудоемкий, но необходимый, поскольку дальнейшее долговременное применение импортного программного обеспечения неминуемо ведет к уязвимости критической информационной инфраструктуры Российской Федерации.

Счетная палата Российской Федерации в 2019 году начала проект отказа от СУБД *Oracle*, выбрав в качестве альтернативы открытую *PostgreSQL*. По словам разработчиков, переход займет достаточно длительное время.

В конце 2023 г. российский государственный концерн «Росатом» сообщил о переводе отраслевой системы электронного документооборота на импортонезависимую отечественную платформу «Атом.Контент». В числе прочего данные из *Oracle Database* были перенесены в российскую СУБД *Postgres Pro* и запущены в промышленную эксплуатацию. При этом были сохранены целевые показатели производительности.

Другая составляющая АИС обусловлена большим объемом обрабатываемых данных. Это приводит к необходимости постройки специальных объектов — центров обработки данных (ЦОД).

В основе ЦОД лежат:

— Информационная инфраструктура, включающая в себя серверное оборудование и обеспечивающая основные функции ЦОД – обработку и хранение данных.

— Телекоммуникационная инфраструктура, обеспечивающая взаимосвязь элементов ЦОД, а также передачу данных между ЦОД и пользователями.

— Инженерная инфраструктура, обеспечивающая нормальное функционирование основных систем ЦОД, которая включает в себя: кондиционирование; бесперебойное электроснабжение; пожарную сигнализацию; систему газового пожаротушения; системы удаленного *IP*-контроля, управления питанием и контроля доступа.

В архитектуре ЦОД выделяют несколько групп серверов:

— Серверы информационных ресурсов, которые должны обрабатывать множество коротких запросов. Следовательно, в архитектуре ЦОД должна быть предусмотрена возможность увеличения количества запросов.

— Серверы приложений, обрабатывающие запросы пользователей, должны иметь возможность увеличения количества выполняемых операций.

— Серверы предоставления информации.

— Служебные серверы.

— Серверы управления системой резервного копирования.

---

[1] Сервис поиска российского ПО для импортозамещения / Реестр программного обеспечения: сайт. — URL: https://reestr.digital.gov.ru/import-substitution/?query=oracle (дата обращения 15.09.2023).

Система хранения данных состоит из элементов памяти, серверов, системы управления и информационно-телекоммуникационной инфраструктуры. Наиболее перспективным решением организации системы хранения данных является технология *SAN*, сочетающая высокую надежность с относительно низкой стоимостью эксплуатации. *SAN* предоставляет возможность соединения любого из серверов с любым элементом памяти, работающим по протоколу *FC*. Технология *SAN* позволяет изменение конфигурации и обслуживание элементов системы без ее остановки. Информационно-телекоммуникационная инфраструктура состоит из волоконно-оптических соединений и коммутаторов, обеспечивающих скорость передачи данных в 200 Мбит/с, что позволяет производить резервное копирование данных в реальном времени.

Оборудование ЦОД должно работать в круглосуточном режиме при заданных температуре и влажности воздуха. Этот режим требует наличия основного и резервного электропитания, систем климатического контроля, обеспечения пожарной и физической безопасности и прочее. Практика показывает, что из 6 000 реальных инцидентов ни одного серьезного пожара в залах с *IT*-оборудованием в ЦОД, соответствующих существующим стандартам, не было зарегистрировано.

По надежности ЦОД классифицируются на:

— Tier 1 – доступность данных 99.671 %;
— Tier 2 – доступность данных 99.741 %;
— Tier 3 – доступность данных 99.982 %;
— Tier 4 – доступность данных 99.995 %.

Мощность, потребляемая ЦОД оценивается в 10 кВт/м^2, что эквивалентно пяти электрочайникам, размещенным на одном квадратном метре и функционирующим в круглосуточном режиме. Помимо того, что эту электроэнергию надо затратить на работу оборудования, ее еще необходимо отвести, чтобы не допустить его перегрева. Потребление электроэнергии одним ЦОД, сопоставимо с потреблением электроэнергии небольшим городом. На сегодняшний день в мире потребление ЦОД электроэнергии оценивается в 3 % от выработки. В связи с увеличением количества ЦОД это соотношение также увеличивается.

Строительство первого ЦОД на территории Российской Федерации было начато в 2016 г., а в 2017 г. он был сдан в эксплуатацию. Местоположение его было выбрано на территории Калининской атомной электростанции в Тверской области, что обеспечило близость линий коммуникаций между Москвой и Санкт-Петербургом, наличие и близость свободных мощностей электропитания, а также охраняемую территорию. Сегодня строительство ЦОД осуществляется на всей территории России. В частности, на севере Карелии и Чукотке, для обеспечения волоконно-оптической линии связи между Мурманском и Владивостоком (со скоростью передачи данных до 200 Тбит/с), прокладываемой по дну Северного Ледовитого океана, для информационного обеспечения Северного морского пути.

В 2020 г. в России было запущено производство микросхем энергонезависимой памяти, созданных на базе технологического процесса 55 нм, энергопо-

требление которых находится на уровне передовых мировых стандартов. К настоящему времени импортозамещение оборудования ЦОД приближается к 100 %.

Одним из основных элементов обеспечения информационной безопасности АИС МВД России, является политика безопасности. Это документ, который содержит: область применения; условия и ограничения; обязанности ответственных должностных лиц; детальное описание нарушений и их последствий; справочную информацию. Эффективность политики безопасности зависит от квалификации и внимательности лиц, реализующих эту политику.

Одной из проблем, стоящих перед любой организацией, является организация доступа к сети «Интернет»: с физической изоляцией; с изоляцией протокола; с маршрутизаторами; со свойствами шлюза.

Наиболее безопасной и простой является модель с физической изоляцией, когда компьютер, с которого осуществляется доступ в интернет, физически отделен от локальной сети. Например, такая модель принята при обработке секретных документов.

Модель изоляции протокола характеризуется возможностью несанкционированного удаленного доступа к данным, а также отсутствием прямого доступа к сети «Интернет» пользователей локальной вычислительной сети.

Модель использования маршрутизаторов применяется в случае к интернету крупной корпоративной сети. В этом случае также имеется возможность несанкционированного удаленного доступа к данным.

Модель подключения к сети «Интернет» через шлюз организуется в аналогичном случае, но при этом вероятность несанкционированного удаленного доступа к данным минимальна.

Шлюз может выполнять несколько функций, в том числе, функцию межсетевого экрана.

Межсетевой экран (МЭ) — это программно-аппаратное устройство, фильтрующее входной и выходной трафик в соответствии с политикой безопасности. Кроме того, в МЭ реализуют средства контроля, аутентификации и обеспечения конфиденциальности информации.

Для МЭ может быть реализован один из следующих подходов:

— Разрешить доступ для сервиса, если он не запрещен политикой безопасности.

— Запретить доступ для сервиса, если он не разрешен политикой безопасности.

Первый подход более уязвим, поскольку предоставляет больше способов обойти МЭ, однако некоторые сервисы фильтровать проблематично, поэтому для них применяется МЭ, реализующий первый подход.

Для обеспечения информационной безопасности обычно используется второй подход, который считается классической моделью доступа. Он более надежен и безопасен, однако его сложнее реализовать, поскольку некоторые сервисы могут оказаться заблокированными или ограниченными.

Вопросы для самоконтроля:

1. Дайте определение жизненного цикла АИС.
2. Какова продолжительность жизненного цикла современных АИС?
3. Назовите основные процессы жизненного цикла АИС.
4. Перечислите проблемы внедрения АИС.
5. Что представляет собой ЦОД?
6. Каковы причины постепенного отказа от импортного ПО?
7. Что такое *Oracle Database*?
8. Что представляет собой ИСОД МВД России?
9. Что такое политика компьютерной безопасности?
10. Что такое межсетевой экран?

§ 3. ИСОД МВД России

Повышение доступности средств *IT* привело к их распространению и в подразделениях МВД России. При этом используемые, как аппаратные, так и программные, платформы в подразделениях МВД России разнились, что порой приводило к невозможности обмена данными между подразделениями. Документы между подразделениями МВД России пересылались телеграммами или факсами. Различное программное обеспечение устанавливалось на АРМ пользователей и на серверах локальных сетей, что обусловливало высокую стоимость обслуживания, низкую надежность и низкую производительность. Существовали и другие проблемы, вызванные отсутствием унификации. Например, исследование, проведенное в ГДР, показало, что в городах с населением свыше 200 000 человек препятствием к успешному использованию ОРИ является децентрализованность картотек и архивов: связи между событиями, лицами и следами, если и выявляются, то слишком поздно.

В 2005 г. МВД России приступило к реализации программы инфраструктурного перевооружения, главной задачей которого являлось создание ведомственной информационно-телекоммуникационной сети — Единой информационно-телекоммуникационной системы (ЕИТКС), на основании которой было бы возможно осуществить интеграцию информационных ресурсов МВД России.

ЕИТКС МВД России — это ведомственная информационно-телекоммуникационная сеть, используемая федеральными органами исполнительной власти Российской Федерации в соответствии с действующими нормативно-правовыми актами. Свободный доступ к ЕИТКС не предусмотрен в целях сохранения государственной тайны и конфиденциальности циркулирующей в ней информации. Связь ЕИТКС с глобальным интернетом реализована через единственный шлюз, что позволяет обеспечить высокий уровень защищенности данных, циркулирующих в ЕИТКС МВД России. В ЕИТКС реализована комплексная защита информации, включающая организационную, техническую и программно-аппаратную, а также криптографическую составляющие средств защиты информации. Это позволило обеспечить связь между всеми подразделениями МВД России, в частности, предоставить доступ к уже существующим АИС. Кроме того, унификация аппаратной и про-

граммной платформ позволила реализовать единую систему электронного документооборота и предоставление государственных услуг в электронном виде.

В нормативных документах можно также встретить аббревиатуру ИМТС — Интегрированная мультисервисная телекоммуникационная система ОВД. Согласно приказу МВД России ИМТС ОВД Российской Федерации является частью ЕИТКС ОВД.

Формирование ЕИТКС было, в основном, закончено к 2014 г.

Реализованные аппаратные и программные решения позволили значительно улучшить характеристики конфиденциальности, целостности и доступности информации, циркулирующей в ЕИТКС. Например, известно только об одном серьезном инциденте, нарушившем целостность данных. 12 мая 2017 г. МВД России подтвердило хакерскую атаку на свои компьютеры, которые находились под управлением операционной системы *Windows*. Своевременно было локализовано около одной тысячи зараженных компьютеров. Остальные ресурсы не подверглись заражению, благодаря использованию иных операционных систем и отечественных серверов с российским процессором «Эльбрус»[1]. В целях обеспечения целостности и конфиденциальности информации в ЕИТКС реализован «Единый контур информационной безопасности».

С 2011 г. началось создание Единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России. Приказом МВД России от 30 марта 2012 г. № 205 была утверждена концепция создания ИСОД МВД России в 2012—2014 годах. Она представляет собой совокупность АИС, программно-аппаратных комплексов и программно-технических средств, а также систем связи и передачи данных, необходимых для обеспечения служебной деятельности ведомства. При этом предполагалась реализация однородных организационных, программных, технических, кадровых и других решений при реализации системного подхода к внедрению АИС в МВД России, что позволяет минимизировать затраты на их приобретение, внедрение и сопровождение на территориально распределенных объектах ОВД. Кроме того, Концепция предусматривала создание единого источника информации для сотрудников подразделений МВД России с учетом разграничения доступа к информационным ресурсам.

В рамках ИСОД были объединены, в числе прочего, существующие АИС МВД России, данные которых размещаются на удаленных серверах (в ЦОД).

Доступ к ИСОД осуществляется с персонального компьютера, подключенного к ЕИТКС. Обмен сообщениями осуществляется с использованием стандартных протоколов сети «Интернет»: *SMTP*, *LMTP*. Доступ пользователей к почтовым сообщениям осуществляется с использованием стандартных протоколов сети «Интернет».

На каждом АРМ сотрудника МВД России, входящем в состав ИСОД, используются средства обеспечения информационной безопасности:

[1] МВД прокомментировало хакерскую атаку на свои серверы / Rbc.ru: сайт. — URL: http://www.rbc.ru/rbcfreenews/5916137e9a794773cd0baea9 (дата обращения: 03.10.2023).

1. Сервис централизованного управления доступом к информационным системам и ресурсам (СУДИС) ИСОД МВД России. Вход сотрудника в операционную систему, установленную на АРМ, должен осуществляться через СУДИС посредством ввода учетной записи.

2. *ViPNetClient* для защиты информации, передаваемой по каналам связи и защиты от сетевых атак.

3. Антивирус Касперского для детектирования вирусов.

4. Агент антивируса Касперского для контроля процессов, инициируемых сетевыми соединениями, и изменяемыми файлами.

5. КриптоПро*CSP* — программное обеспечение для работы с электронной подписью.

6. Отчуждаемый носитель, содержащий ключ электронной подписи, связанный с персональной учетной записью сотрудника МВД России в СУДИС, и иную информацию, сертифицированный ФСТЭК России. Это дополнительное программно-аппаратное средство криптографической защиты информации, которое позволяет также блокировать доступ к информации при его извлечении.

7. Пароль, связанный с персональной учетной записью сотрудника МВД России в СУДИС.

Сотрудник МВД России несет персональную ответственность за инциденты информационной безопасности ИСОД МВД России, произошедшие в результате использования его учетной записи в СУДИС.

Сотрудникам МВД России категорически запрещается:

— сообщать пароль кому-либо;

— хранить пароль в доступном для других лиц месте;

— пересылать пароль по открытым каналам связи;

— использовать учетные записи других сотрудников;

— вводить пароль в условиях его возможной компрометации.

Кроме того, в целях обеспечения при работе с ИСОД МВД России пользователям запрещается:

— использование не разрешенных носителей информации;

— открывать вложения и читать электронную почту, пришедшую от неизвестного отправителя;

— осуществлять служебную переписку с иных кроме @mvd.ru почтовых адресов.

Отдельные требования для обеспечения информационной безопасности сформулированы при доступе к ИСОД МВД России с мобильных устройств.

Структуру ИСОД можно представить в виде трех разделов: сервисы повседневной деятельности; сервисы межведомственного взаимодействия и оказания государственных услуг; сервисы оперативно-служебной деятельности.

Сервисы повседневной деятельности включают в себя:

— Сервис электронного документооборота (СЭД), предназначенный для обеспечения электронного документооборота между сотрудниками.

— Сервис электронной почты (СЭП), предназначенный для обмена электронными сообщениями. По функциональным возможностям СЭП бли-

зок к обычной электронной почте. Доступна версия для мобильных персональных устройств.

— Сервис видеоконференцсвязи (СВКС-М), предназначенный для создания канала видеоконференцсвязи между сотрудниками МВД России.

— Ведомственный информационный портал (ВИСП), обеспечивающий доступ к справочной информации по ИСОД МВД России; доступ к сведениям об организационно-штатной структуре МВД России; доступ к адресно-телефонному справочнику МВД России.

Сервисы межведомственного взаимодействия и оказания государственных услуг включают в себя:

— Сервис предоставления государственных услуг (СПГУ) предназначен для обеспечения взаимодействия с гражданами и межведомственного взаимодействия в рамках предоставления государственных услуг, которые включают в себя: государственные услуги по линии информационно-справочной работы; государственные услуги по линии обеспечения безопасности дорожного движения; государственные услуги в сфере миграции; государственные услуги по линии контроля за оборотом наркотиков; государственную услугу по проведению добровольной дактилоскопической регистрации; электронные заявления.

— Система централизованного учета оружия (СЦУО) содержит данные о нарезном боевом, служебном, гражданском оружии, гранатометах, реактивных пехотных огнеметах, переносных зенитно-ракетных и противотанковых комплексах, учтенных в МВД России.

— Сервис «Модернизация ИБД», предназначенный для повышения эффективности оперативно-служебной деятельности ОВД при формировании, ведении и использовании централизованных учетов.

— Сервис «Ретроспектива», предназначенный для предоставления информации о реабилитации жертв политических репрессий.

Сервисы оперативно-служебной деятельности включают в себя:

— Сервис обеспечения деятельности подразделений тылового обеспечения (СОМТО).

— Сервис оформления проезда сотрудников (СОПС).

— Сервис обеспечения экономической безопасности (СОЭБ), предназначенный для обработки ОРИ в подразделениях экономической безопасности.

— Федеральная информационная система ГИБДД МВД России (ФИС ГИБДД–М, «Паутина», ЕАИСТО, АИПС «Автопоиск», АИПС «Ограничения»). С апреля 2022 г. создается единая цифровая платформа ГИБДД МВД России.

— Централизованная интегрированная автоматизированная дактилоскопическая информационная система МВД России (ЦИАДИС).

— Сервис «Следопыт-М», предназначенный для предоставления сведений о документах, удостоверяющих личность граждан.

— Сервис обеспечения деятельности дежурных частей (СОДЧ).

— Сервис обеспечения охраны общественного порядка (СООП).

— АИС генетической информации «Ксенон–2».

— Единая АИС экспертно-криминалистической деятельности.

— МОСТ — сервис статистической отчетности МВД России.

— Сервис обеспечения оперативно-служебной деятельности НЦБ Интерпола МВД России (СОДИ).

Кроме того, в ИСОД доступны:

— Сервис обеспечения государственной защиты лиц (СУОГЗ).

— Сервис ГУ Собственной безопасности МВД России (СОПДГУСБ).

— Сервис обеспечения кадровой деятельности (СОКД) предназначен для учета кадров и прохождения службы в ОВД;

— Сервис обеспечения деятельности организационно-штатных подразделений (СОШП).

— Сервис обеспечения деятельности правовых подразделений системы МВД России (СОДПП).

— Сервис автоматизированной проверки граждан, транспортных средств и документов на объектах учетно-заградительной системы подразделений МВД России (САПДУЗС).

— Сервисы Главного управления по вопросам миграции (ГУВМ).

— Сервис для автоматизации деятельности Центров автоматизированной фиксации административных правонарушений в области дорожного движения (ЦАФАП) предназначен для вынесения решения по административным нарушениям, зафиксированным в автоматическом режиме с помощью специальных технических средств.

Разработка и успешная эксплуатация ИСОД МВД России среди систем, сопоставимых по масштабу, оценивается[1] как одна из самых успешных в мире. В США, например, подобный проект был заморожен из-за технических сложностей и высокой стоимости реализации.

Вопросы для самоконтроля:

1. Что такое ЕИТКС МВД России?
2. Каковы цели и задачи ЕИТКС МВД России?
3. Какова структура ЕИТКС МВД России?
4. В чем отличие ИМТС от ЕИТКС МВД России?
5. Когда было начато формирование ЕИТКС МВД России?
6. Что такое ИСОД МВД России?
7. Когда было начато формирование ИСОД МВД России?
8. Какова структура ИСОД МВД России?
9. Какие сервисы ИСОД МВД России Вы знаете?

[1] Система для полицейских: что представляет собой ИСОД МВД России / Cnews: сайт. — URL: https://www.cnews.ru/articles/2018-03-23_sistema_dlya_politsejskih_chto_predstavlyaet_soboj_isod_mvd_rossii (дата обращения: 29.09.2023).

Заключение

Информация — это сведения, из которых формируются знания, а, впоследствии, может сформироваться и понимание того, что происходит в интересующей ситуации. Понимание же позволяет с высокой вероятностью прогнозировать развитие событий и предпринимать шаги, которые приведут к достижению поставленной цели.

Сказанное в полной мере относится и к правоохранительной деятельности. Обладание информацией приводит к более успешному достижению целей. За 3400 лет, прошедших с первого известного криминалистического учета, в этой области ничего не изменилось. Более того, процесс всестороннего развития человеческого общества, в том числе, наступление информационной эры, только ярче высветил необходимость накопления и обработки поступающей информации.

На сегодняшний день, благодаря осуществленным усилиям, большую часть информации, необходимой для успешного осуществления оперативно-розыскной деятельности, удалось сконцентрировать в автоматизированных информационных системах, функционирующих в рамках ИСОД — Единой системы информационно-аналитического обеспечения деятельности МВД России.

В представленном издании описаны краткая история развития и современное состояние дел в области сохранения, обработки и выдачи криминалистически значимой информации в МВД России. Уделено внимание вопросам обеспечения конфиденциальности, целостности и доступности информации, обрабатываемой в современных автоматизированных информационных системах.

Список рекомендуемых источников

Нормативные правовые акты:

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.; с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Об оперативно-розыскной деятельности в Российской Федерации: федеральный закон от 12.08.1995 г. № 144-ФЗ.

3. О государственной дактилоскопической регистрации в Российской Федерации: федеральный закон от 25.07.1998 г. № 128-ФЗ

4. О связи: федеральный закон от 07.07.2003 г. № 126-ФЗ.

5. Об информации, информационных технологиях и о защите информации: федеральный закон от 27.06.2006 г. № 149-ФЗ.

6. О полиции: федеральный закон от 07.02.2011 г. № 3-ФЗ.

7. О едином федеральном информационном регистре, содержащем сведения о населении Российской Федерации: федеральный закон от 08.06.2020 г. № 168-ФЗ.

8. Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации в целях обеспечения функционирования сетей связи специального назначения: постановление Правительства Российской Федерации от 22.02.2006 г. № 103.

9. О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации: постановление Правительства Российской Федерации от 23.09.2020 г. № 1526.

10. Об утверждении Типового положения об информационном центре МВД, ГУВД, УВД субъекта Российской Федерации, УВДТ, ГУВДРО СОБ МВД России: приказ МВД России от 28.03.2002 г. № 288.

11. Об утверждении структуры Интегрированной мультисервисной телекоммуникационной системы ОВД: приказ МВД России от 26.09.2006 г. № 763.

12. Об утверждении Порядка формирования направляемой в органы внутренних дел дактилоскопической информации: приказ МВД России № 659, МЧС России № 717, МО России № 473, Минфина России № 208н, МЮ России № 209, Минтранса России № 385, СВР России № 63, ФСБ России № 429, ФСО России № 376, ФСВНГ России № 145, ГУСПП России № 299, ГП России, СК России от 23.09.2020 г.

13. ГОСТ Р ИСО/МЭК 12207:2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств»

Основная литература:

14. Овчинский С. С. Оперативно-розыскная информация / под редакцией А. С. Овчинского и В. С. Овчинского. — Москва: ИНФРА-М, 2000. — 367 с.

Дополнительная литература:

15. Бреслер Ф. Интерпол. — Москва: Центрполиграф, 1996. — 406 с.

16. Галвазин С. Н. Охранные структуры Российской империи. Москва: Коллекция «Совершенно секретно», 2001. — 191 с.

17. Информационные технологии управления и организация защиты информации: курс лекций / В. А. Апульцин, Ш. Х. Гонов, В. Н. Лебедев, В. Ю. Петрова. — Москва: Академия управления МВД России, 2021. — 72 с.

Интернет-источники:

18. Видеофильм. Теория правды. Честность — основной элемент. URL: https://ya.ru/video/preview/8711839519449178540 (дата обращения 01.10.2023).

19. Основные задачи ГИАЦ МВД России /МВД России: официальный сайт. — URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Centri/Glavnij_ informacionno_analiticheskij_cen/Ustav?ysclid=lmg9486rif694914277 (дата обращения: 12.09.2023).

20. Перечень отдельной медицинской учетной документации, используемой в лечебно-профилактических учреждениях Доступ из ИПП «Гарант.ру»: сайт. — URL: http://base.garant.ru/52490030/ (дата обращения: 12.09.2023).

21. Структура ГИАЦ МВД России /МВД России: официальный сайт. — URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Centri/Glavnij_informacionno_ analiticheskij_cen/Struktura_FKU_GIAC_MVD_Rossii?ysclid=lmg8zgi11c113972542 (дата обращения: 12.09.2023).

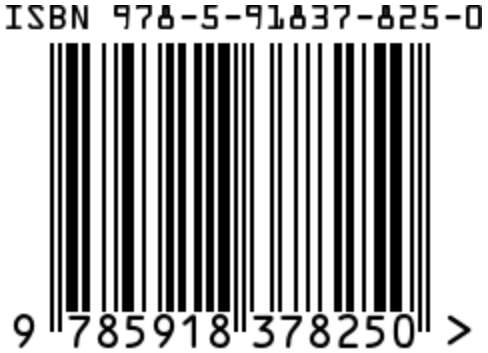
Учебное издание

Якушев Денис Игоревич,
доктор технических наук

СПЕЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Учебно-методическое пособие

Редактор *Лукьянова Г. В.*
Компьютерная вёрстка *Душкова А. Ю.*
Дизайн обложки *Шеряй А. Н.*



EDN: RIWEVY

Подписано в печать 06.05.2024. Формат 60x84 $^{1}/_{8}$
Печать цифровая. Объем 3,0 п. л. Тираж 100 экз. Заказ № 38/24

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1