ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Уфа 2022

УДК 351.74.07:004(470)(075.8)
ББК 67.401.133-8(2Рос)с51я73-1
И74

Рекомендовано к опубликованию
редакционно-издательским советом Уфимского ЮИ МВД России

Рецензенты:
доктор технических наук, профессор М. Б. Наумов
(Нижегородская академия МВД России);
кандидат юридических наук Е. Ю. Семенов
(Орловский юридический институт МВД России имени В. В. Лукьянова)

Коллектив авторов:
В. В. Антонов – доктор технических наук, профессор;
З. И. Харисова – кандидат технических наук, б/з;
Н. Р. Калимуллин – б/с, б/з;
И. Н. Губайдуллина – кандидат экономических наук, доцент;
А. Ф. Острякова – кандидат экономических наук, б/з

И74 **Информационные технологии в управлении органами внутренних дел** : учебное пособие / В. В. Антонов [и др.]. – Уфа : Уфимский ЮИ МВД России, 2022. – 48 с. – Текст : непосредственный.

ISBN 978-5-7247-1108-1

В учебном пособии представлен процесс внедрения современных информационных технологий в системе органов внутренних дел, особенности управления базами данных, формирование рекомендаций для повышения эффективности управления в органах внутренних дел на основе современных методов интеллектуализации и автоматизации.

Предназначено для обучающихся образовательных организаций МВД России.

УДК 351.74.07:004(470)(075.8)
ББК 67.401.133-8(2Рос)с51я73-1

ISBN 978-5-7247-1108-1

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Под понятием «управление» в настоящее время подразумевают относительно молодое направление, в основе которого лежит сбор, анализ и распределение информации. Управление так же подразумевает под собой организацию и контроль планирования, распространение, структурирование и мониторинг информации с целью прогнозирования определенных ожиданий, а также информационного обеспечения конкретных систем.

В соответствии со сложившимися информационными связями в органах внутренних дел (далее – ОВД), а также характером и степенью их важности, целостности, достоверности и надежности целесообразно рассмотрение такого направления, как управление в ОВД. Как показывает практика – отсутствие рациональных схем организации информационных потоков приводит к огромным издержкам и затратам на поддержание необходимой полноты, актуальности и своевременности предъявления информации.

Сферу управления ОВД можно описать как совокупность всех необходимых для этого решений на всех этапах жизненного цикла объекта управления, включающую все действия и операции, связанные как с информацией во всех её формах и состояниях, так и с объектом в целом. При этом должны решаться задачи определения ценности и эффективности использования самой информации так, чтобы каждый сотрудник ОВД получал только релевантную информацию, но из других ресурсов, в той или иной мере входящих в контакт с информацией: управленческих, кадровых, финансовых и т. д.

Задачами информационного управления являются:

– формирование у обучающихся современного управленческого мышления с учетом использования информационных технологий;

– выработка практических навыков анализа и решения управленческих проблем в органах внутренних дел;

– изучение методов управления организацией и практических способов их применения.

В пособии представлен анализ внедрения современных информационных технологий в системе ОВД, особенности управления базами данных, формирование рекомендаций для повышения эффективности управления в ОВД на основе современных методов интеллектуализации и автоматизации.

Данное учебное пособие предназначено для повышения эффективности работы сотрудников ОВД с современными информационными технологиями в профессиональной деятельности и повышения эффективности управления в области противодействия отдельным видам преступления.

ГЛАВА 1. ПОНЯТИЕ, ЗНАЧЕНИЕ И ПРИНЦИПЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В УПРАВЛЕНИИ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ

§ 1. Информационное общество и инструментарий информационных технологий

В основе взаимоотношений человека с окружающим его миром и обществом лежат информационные процессы. Каждый такой процесс включает соответствующие адекватные методы, позволяющие воспринять данные, передаваемые посредством телевидения, радиопередач и интернет-ресурсов.

В истории человечества выделяют три социально-технологические фазы: аграрная, индустриальная и информационная. Экономическая деятельность в аграрном обществе была связана с производством продуктов питания, в индустриальном обществе – с производством промышленных товаров. Информационное общество является новой исторической фазой развития цивилизации, в которой главными продуктами выступают информация и знания. Отличительные черты информационного общества:

– возрастающая доля информационных коммуникаций;

– глобальное информационное пространство, обеспечивающее людям эффективное информационное взаимодействие;

– доступ к мировым информационным ресурсам;

– удовлетворение потребностей в информационных продуктах.

Появление и стремительное распространение Интернета по времени неслучайно совпало с переходом к информационному обществу.

Необходимо отметить, что в наши дни возникает новая индустрия переработки информации на базе компьютерных и информационно-телекоммуникационных технологий. Информация перерабатывается с помощью аппаратного и программного обеспечения данного процесса. Из этих средств можно отдельно выделить программные средства, служащие программным инструментарием информационных технологий.

Так, в России согласно утвержденному плану перехода на отечественное офисное программное обеспечение до конца 2018 года федеральные органы исполнительной власти должны были осуществить переход на отечественные программные продукты[1]. Для субъектов Российской Федерации, органов местного самоуправления, государственных компаний и корпораций ставилась задача подготовить соответствующие методические рекомендации с плановым сроком решения задачи к 2020 году, однако на

[1] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г. : утв. Президентом РФ 24 июля 2013 г. № Пр-1753) // Доступ из справ.-правовой системы «КонсультантПлюс».

сегодняшний день можно обозначить ряд проблем, которые способствуют сдвигу плановых сроков[1].

В первую очередь это обусловлено недостаточным финансированием для столь масштабного проекта замещения в относительно сжатые сроки. Далеко не все отечественное программное обеспечение предлагается для использования на безвозмездной основе за исключение ряда усеченных версий или версий для использования в учебных целях. Кризис на финансовом рынке, валютная нестабильность, всеобщий недостаток оборотных средств оказывают на это существенное влияние.

Кроме того, целесообразно рассмотрение вопроса о нехватке квалифицированных кадров как в области разработки[2], так и в области непосредственного вывода продуктов на российский рынок. В свою очередь, помимо конкурентоспособности важна надежность и безопасность разрабатываемых продуктов с целью обеспечения должного уровня информационной безопасности страны.

Развитие компьютерных и информационно-телекоммуникационных технологий является в первую очередь государственной стратегией, которая представляет из себя программу экономической эволюции страны, включающую в себя комплекс мероприятий, которые способны снизить зависимость отечественной экономики от импортных продуктов. Потребность в разработке системы импортозамещения является основой для формирования нового механизма, направленного на повышение эффективности деятельности путем замещения импортных составляющих, материалов, технологий, оборудования и программных средств, в том числе на соответствующие товары российского производства, а также на оценку уровня осуществляемых мероприятий и выявления недостатков.

Введение санкционной политики как раз поспособствовало активизации этого процесса. Российская экономика оказалась перед необходимо-

---

[1] План импортозамещения программного обеспечения, утвержден приказом Минкомсвязи России от 1 апреля 2015 г. № 96 в целях реализации пункта 41 плана первоочередных мероприятий по обеспечению устойчивого развития экономики и социальной стабильности в 2015 г., утвержденного распоряжением Правительства Российской Федерации от 27 января 2015 г. № 98-р, формирования благоприятных условий для развития разработки отечественного конкурентоспособного программного обеспечения, учитывая предложения заинтересованных российских организаций отрасли информационных технологий и их объединений (ассоциаций) // Центр мониторинга технологической модернизации и научно-технического развития. Информационный портал, Российская Федерация, 2021. – URL: http://cmntr.ru/standards/detail.php?ID=306&sphrase_ id=15897 (дата обращения: 11.01.2022)

[2] Харисова З. И. Международно-правовые основы информационной безопасности в Целях устойчивого развития // Правовое обеспечение развития социального государства в свете целей устойчивого развития : сборник материалов Международной научно-практической конференции (Уфа, 12–13 ноября 2018 г.). В 2-х ч. : ч. 2. – Уфа : РИЦ БашГУ, 2018. – С. 103–106.

стью за короткий срок совершить значительный шаг в сторону реализации конкурентоспособности, на который в иных условиях, возможно, понадобилось бы длительное время. Не остались в стороне и федеральные органы исполнительной власти, деятельность которых тесно связана с использованием инфокоммуникационных технологий и информационных систем на базе Windows.

Поскольку политика импортозамещения во многом обусловлена необходимостью обеспечения национальной безопасности, важно определить приоритеты в разработке отечественного программного обеспечения с позиции какого класса и для каких отраслей следует его разрабатывать.

Требования клиентов к программному обеспечению возрастают: они ждут от отечественных решений более серьезных возможностей на перспективу, по сравнению с имеющимся западным программным обеспечением – иначе у потребителя напрочь будет отсутствовать мотивация перехода, как минимум по причине необходимости восприятия нового интерфейса. При этом внедрение продвинутых решений – принципиально новая задача, в том числе и для самих заказчиков, она требует больше усилий, больших временных затрат, а также дополнительного финансирования, что способствует затягиванию во времени внедрения отечественных продуктов.

Рассмотрев, пожалуй, одну из сложнейших задач – переход на отечественную операционную систему Astra Linux, которая на сегодняшний день одобрена ФСБ России, Минобороны и Федеральной службой по техническому и экспортному контролю России, стоит отметить, что система позволяет обрабатывать информацию ограниченного доступа вплоть до степени секретности «Совершенно секретно» в автоматизированных системах министерств, ведомств и компаний с повышенными требованиями к информационной безопасности, что является весьма конкурентоспособной возможностью. Операционная система включена в стандарты государственных корпораций «Росатом» и «Ростех», принята на снабжение в Вооруженных Силах Российской Федерации и активно на сегодняшний день внедряется в органы государственного управления, ведомства и государственные корпорации.

Первые поставки продукта для министерств были проведены еще в 2010 году. В текущем же году Вооруженными силами было принято решение полностью перейти на Astra Linux. Необходимо, однако, отметить что существует ряд проблем при использовании данной системы. Например, в операционной системе Astra Linux Special Edition версии 1.3, установленной на компьютер со встроенной видеокартой Intel, в некоторых случаях могут проявиться графические артефакты. На текущий момент собрано несколько видеодрайверов для возможного решения этой проблемы. Часть пакетов уже могут функционировать в режиме замкнутой программной среды.

Существенным недостатком рассматриваемой операционной является значительно меньшее, чем для платформы Windows, количество совместимых прикладных программ. Более того, если речь идет о программах безусловно лидирующих по тому или иному прикладному аспекту, то в операционной системе Linux зачастую отсутствуют соответствующие версии данных программ, сопоставимые по функциональным возможностям.

К таким прикладным программам относятся продукты компании Adobe, инструментальные пакеты 1С, программы инженерного проектирования AutoCAD, большинство программ распознавания текстов, специализированное программное обеспечение, в том числе системы узкого назначения, разработанные в ОВД.

Безусловно, в операционной системе Linux есть и графические редакторы, программы моделирования и проектирования, однако, большинство из них значительно уступают лидерам-разработчикам программных продуктов в семействе операционных систем Windows.

Среднестатистические данные показывают (рис. 1), что доля операционных систем семейства Windows только растет, среднее количество пользователей системы Linux составляет около 2 %. За несколько последних лет операционная система Linux понемногу, но все же набирает популярность[1]. Однако для полного перехода на новую операционную систему необходимо решение попутных проблем импортозамещения программного и аппаратного обеспечения, что требует значительных усилий и вложений[2].

На сегодняшний день переход от индустриальной к информационно-технологической эпохе стал последствием информатизации и компьютеризации практически всех сфер жизнедеятельности человека. Современные электронные вычислительные машины могут считывать и передавать цифровую информацию без непосредственного участия оператора. Эволюция человечества неизбежно приводит к необходимости создания, а также массового использования технологий искусственного интеллекта (далее – ИИ), которые в будущем будут способствовать решению различных научно-технических задач.

---

[1] Market Share Statistics for Internet Technologies // Информационный портал о статистике использования интернет-технологий. – URL : https://www.netmarketshare.com/operating-system-market-share.aspx (дата обращения: 11.01.2022).

[2] План импортозамещения программного обеспечения (Сегменты рынка корпоративного программного обеспечения), Приложение к приказу Министерства связи и массовых коммуникаций Российской Федерации от 1 апреля 2015 года №96 // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации. – URL : https://digital.gov.ru/uploaded/files/plan–importozamescheniya.pdf (дата обращения: 26.01.2022).

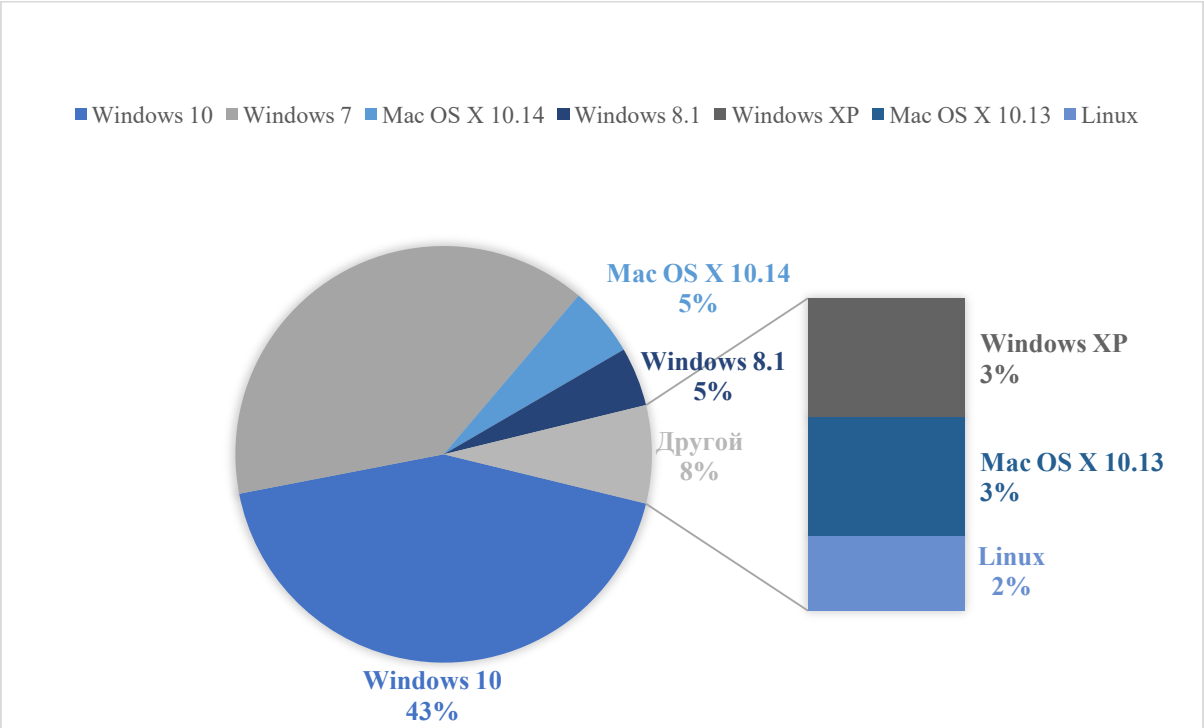

Рис. 1. Среднестатистические данные использования операционных систем в мировом масштабе

Необходимо отметить, что в настоящее время ИИ развивается повсеместно, так, в некоторых странах данная технология зачастую приходит на смену традиционным системам обработки данных информации, кроме того, известен ряд случаев использования ИИ на службе в полиции так, например, в ряде стран технологии ИИ внедряются в виде роботов-полицейских. На данный момент ведется активное применение ИИ с целью оказания помощи правоохранительным органам в служебной деятельности. Хотелось бы отметить, что на сегодняшний день элементы ИИ зачастую применяются для минимизации трудовых ресурсов, численности людей при решении различных задач в том числе в борьбе с преступностью. Известна возможность использования так называемые «умных» очков с функцией распознавания лиц для поиска преступников. Создаваемые системы на основе нейронных сетей (далее − НС) способны анализировать события и осуществлять поиск преступников по материалам среди всех жителей государства. Так, внедряемые видеосистемы с использованием НС распознают преступников по их анатомическим признакам, в том числе среди толпы людей. Но необходимо помнить, что внедрение в работу правоохранительных органов систем ИИ на сегодняшний день не может исключать сбои в работе машин, так же необходимо учесть тот факт, что у робота нет чувств и эмоций, способствующих иногда объективной оценке сложившейся ситуации и объективному решению той или иной задачи.

Следует сказать, что развитию искусственного интеллекта присущ как ряд положительных, так ряд и отрицательных особенностей, которые в том числе порождают новые виды угроз. Так, велика вероятность беспрепятственного взлома и продаж баз данных систем ИИ. Зачастую разработка систем на основе осуществляется на базе систем открытого доступа. Например, беспилотный летательный аппарат, разработанный с использованием НС, может являться центром управления подобных летательных аппаратов, а в ряде стран они применяются государственными структурами для осуществления задач в области противодействия преступникам, преступным организациям в сфере оборота наркотиков или, к примеру, доставки различных запрещенных предметов в места лишения свободы.

При применении интеллектуальных систем в правоохранительной деятельности есть риск столкнуться с таким фактором, как излишнее доверие алгоритму машиной системы без учета соответствия реальному применению информации, поэтому об окончательном и повсеместном переходе на системы ИИ речи на сегодняшний день быть не может.

В приведенных выше примерах использования ИИ видно, что на сегодняшний день имеется проблема, заключающаяся в том, что совершенные преступления с использованием нейронных технологий во всех их вариациях отличаются сложностью и высокой степенью скрытности, что весьма усложняет их раскрываемость, кроме того, отдельного внимания заслуживает правовое регулирование искусственного интеллекта и определение его статуса как «электронного лица»[1].

Основными направлениями повышения доступности и качества данных, необходимых для развития ИИ, в настоящее время являются: разработка унифицированных методологий, а также осуществление контроля за соблюдением указных методологий; создание и развитие инфраструктур для обеспечения доступа к наборам данных. Для реализации подобной стратегии возникает необходимость в создании нормативно-правовой базы, контролирующей обеспечение защиты данных.

Использование ИИ повсеместно позволяет грамотно планировать и прогнозировать управленческие решения, оптимизировать обработку больших данных, автоматизировать технологические процессы, использовать автономные (полностью автоматические) системы и комплексы в различных отраслях промышленности. ИИ создают благоприятные ус-

[1] О развитии искусственного интеллекта в Российской Федерации : указ Президента Российской Федерации от 10 октября 2019 г. № 490 // Официальный интернет-портал правовой информации. – URL : http://publication.pravo.gov.ru/Document/View/0001201910110003 (дата обращения: 26.01.2022).

ловия и облегчают работу не только в правоохранительных органах, но и в других сферах[1].

При всех положительных моментах использования ИИ имеются так же и недостатки, как в применении в правоохранительных органах, так и в применении в различных сферах жизнедеятельности человека: в промышленности, медицине, экономике и т. п.[2] В связи с этим на сегодняшний день замена человека на электронно-вычислительные машины, обладающие ИИ, нецелесообразно, но использовать их в качестве вспомогательного средства для осуществления и решения рутинных задач вполне реально. По этой причине в системе МВД России, а также в сфере образования и науки возникает большая необходимость в повышении квалификации в области применения систем на основе ИИ, совершенствовании навыков специалистов в области информационных технологий, увеличения численности кадров, предназначенных для эффективной борьбы с преступлениями, связанными с применением высоких технологий.

§ 2. Роль информации в управлении органами внутренних дел

Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» в ст. 10 «Информационное обеспечение и документирование оперативно-розыскной деятельности» гласит, что органы, осуществляющие оперативно-розыскную деятельность, для решения задач, возложенных на них, могут создавать и использовать информационные системы, а также заводить дела оперативного учета.

Информация, используемая в органах внутренних дел, содержит сведения о состоянии преступности и общественного порядка на обслуживаемой территории, о самих органах и подразделениях, их силах и средствах. В дежурных частях, у оперативных сотрудников, участковых уполномоченных полиции, следователей, сотрудников экспертно-криминалистических подразделений, других подразделений в документах первичного учета, в учетных журналах и на других носителях накапливаются массивы данных оперативно-розыскного и оперативно-справочного назначения, в которых содержатся сведения:

– о правонарушителях и преступниках;

---

[1] Лонщакова А. Р., Харисова З. И., Антонов В. В. Обеспечение достоверности и информационной безопасности проведения психофизиологических исследований в рамках уголовного судопроизводства в Российской Федерации и за рубежом // Евразийский юридический журнал. – 2019. – № 9 (136). – С. 240–242.

[2] Kharisova Z. I., Fetisov V. S., Dmitriyev O. A., Melnichuk O. V. Rapid particle size analysis of suspensions based on video technology and artificial neural network with additional training during operation // International Journal of Applied Engineering Research RI Publications. – 2017. – Vol. 12. – №.7. – P. 1271–1278.

– о владельцах автомототранспортных средств;
– о владельцах огнестрельного оружия;
– о событиях и фактах криминального характера, правонарушениях;
– о похищенных и изъятых вещах, предметах антиквариата;
– а также другая информация, подлежащая хранению.

Службы и подразделения органов внутренних дел характеризуются данными: о силах и средствах, которыми располагает орган; о результатах их деятельности.

Перечисленные выше сведения используются при организации работы подразделений и принятии практических мер по борьбе с преступностью и правонарушениями.

В информационном обеспечении ОВД центральное место занимают учеты, которые используются для регистрации первичной информации о преступлениях и лицах, их совершивших.

Учет подследственных МВД России преступлений охватывает 95 % криминальных проявлений и дает достаточно полную картину оперативной обстановки в стране и ее регионах.

Главный информационный центр – самый крупный банк оперативно-справочной и розыскной информации в системе МВД России. На него возложена задача обеспечения органов и учреждений внутренних дел различной информацией – статистической, розыскной, оперативно-справочной, криминалистической, производственно-экономической, научно-технической, архивной. Это уникальные, многопрофильные централизованные массивы информации, в целом насчитывающие около 50 млн учетных документов.

Информационные центры МВД являются важнейшим звеном в системе информационного обеспечения в управлении ОВД Российской Федерации. На них ложится основная нагрузка в обеспечении информационной поддержки ОВД в раскрытии и расследовании преступлений, розыске преступников.

Информационные центры являются головными подразделениями в системе МВД в области информатизации: обеспечении статистической, оперативно-справочной, оперативно-розыскной, криминалистической, архивной и иной информацией, а также компьютеризации и построения региональных информационно-вычислительных сетей и интегрированных банков данных.

С помощью учетов получается информация, которая помогает в раскрытии, расследовании и предупреждении преступлений, розыске преступников, установлении личности неизвестных граждан и принадлежности изъятого имущества.

Наряду с учетами в органах внутренних дел ведутся экспертно-криминалистические централизованные коллекции и картотеки, которые создаются и хранятся в экспертно-криминалистических центрах (далее –

ЭКЦ) МВД России (федеральные) и экспертно-криминалистических управлениях (далее – ЭКУ) МВД России. Коллекции и картотеки ЭКУ и ЭКЦ ориентированы прежде всего на обеспечение раскрытия и расследования преступлений.

Накапливаемая в учетах, коллекциях и картотеках оперативно-справочная, розыскная и криминалистическая информация, именуется криминальной.

Учеты классифицируются по функциональному и объектовому признакам.

Функционально учеты разделяются на оперативно-справочные, розыскные и криминалистические.

По объектовому признаку учеты разделяют на три группы: лиц, преступлений (правонарушений), предметов.

Информационная база системы МВД России построена на принципе централизации учетов. Ее составляют оперативно-справочные, розыскные и криминалистические учеты и картотеки, сосредоточенные в ГИЦ МВД России и ИЦ МВД, УВД, УВДТ, и локальные учеты горрайлинорганов. В целом их массивы оцениваются примерно в 250–300 млн учетных документов.

Централизованные оперативно-справочные, розыскные и криминалистические учеты располагают следующими сведениями об осужденных гражданах России, иностранцах и лицах без гражданства:

– судимость, место и время отбывания наказания, дата и основание освобождения;

– перемещение осужденных;

– смерть в местах лишения свободы, изменение приговора, амнистия, номер уголовного дела;

– место жительства и место работы до осуждения;

– задержание за бродяжничество;

– группа крови и дактилоформула осужденных.

Дактилоскопический учет позволяет устанавливать личность преступников, арестованных, задержанных, а также неизвестных больных и неопознанных трупов.

Учеты ОВД в зависимости от способа обработки информации подразделяются на три вида: ручные, механизированные, автоматизированные.

Автоматизированные учеты состоят из ряда автоматизированных информационно-поисковых систем (далее – АИПС). Накопление и обработка криминальной информации с помощью АИПС осуществляются в региональных банках криминальной информации (РБКИ).

Эффективность борьбы с преступностью определяется уровнем организации оперативной, следственной, профилактической работы, проводимой ОВД.

В свою очередь, результаты этой работы зависят от качества информационной поддержки, поскольку основные усилия практических работников в расследовании, раскрытии и предотвращении преступлений так или иначе связаны с получением необходимой информации, именно эти функции и призваны обеспечить систему информационного обеспечения ОВД, которая поддерживает в настоящее время значительный объем информации.

Такой подход может сделать невозможным в дальнейшем реализацию единого информационного пространства.

В целом в органах внутренних дел России в автоматизированном режиме с помощью ЭВМ обрабатываются задачи оперативно-розыскного и справочного назначения, а также задачи учетно-статистического, управленческого и производственно-экономического назначения.

Сейчас большинство регионов России приступило к созданию региональных информационных систем, но эти процессы пока еще носят стихийный характер. Разрабатываемые системы зачастую реализуют собственный язык манипулирования данными, свои потоки и форматы данных, свои решения в части архитектуры и выбора технических средств.

§ 3. Применение современных информационных технологий в управлении органами внутренних дел

Сотрудникам ОВД с момента вступления в силу Федерального закона РФ от 7 февраля 2011 г. № 3-ФЗ «О полиции»[1], вменяется в обязанность использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру.

В рамках внедрения информационных технологий в деятельность ОВД России Указом Президента РФ от 1 марта 2011 г. № 248 «Вопросы Министерства внутренних дел Российской Федерации»[2] в структуре МВД России создан Департамент информационных технологий, связи и защиты информации МВД России, основными задачами которой являются:

– совершенствование информационных и телекоммуникационных технологий;

– совершенствование автоматизированных информационных систем;

– развитие современных цифровых систем связи;

---

[1] О полиции : федеральный закон от 7 февраля 2011 г. № 3-ФЗ : принят Государственной Думой 28 января 2011 г. : одобрен Советом Федерации 2 февраля 2011 г. // Собрание законодательства РФ. – 2011. – № 7. – Ст. 900.

[2] Вопросы Министерства внутренних дел Российской Федерации : указ Президента РФ от 1 марта 2011 г. № 248 // Российская газета. – 2011. – № 43. – С. 7–9.

– противодействие техническим разведкам;

– техническая защита информации;

– формирование и ведение информационных ресурсов;

– межведомственное информационное взаимодействие;

– реализация государственных и ведомственных программ в рамках информатизации и другие задачи.

Так, в ряде регионов прошло испытание системы передачи данных по защищенному каналу удаленного мобильного доступа на базе планшетного компьютера «Барс». Данная система позволяет сотрудникам получать оперативную и достоверную информацию о гражданах, автомобилях, информацию о розыске из информационных систем МВД России.

В деятельности подразделений ОВД может использоваться различное программное обеспечение (универсальное, специальное).

Универсальные программы (информационно-поисковые системы, редакторы, электронные таблицы и т. п.) общего назначения не только повышают производительность труда и эффективность работы по выявлению, раскрытию и расследованию преступлений, но и поднимают ее на качественно новый уровень.

Специализированные программы могут быть ориентированы на непосредственное их применение при осуществлении оперативно-розыскных мероприятий в направлении борьбы с информационной (в том числе компьютерной) преступностью.

Поисковые программные средства могут найти широкое применение в оперативно-розыскной деятельности (непроцессуальная форма), в том числе и до возбуждения уголовного дела. Факт обнаружения объектов (программ закладок, программного обеспечения для изготовления вирусов или для осуществления взлома компьютерных сетей и т. п.) может послужить основанием для возбуждения дела и производства расследования.

В процессуальной форме поисковые программные средства могут найти применение при проведении следственных действий, таких как следственный осмотр (все его виды), выемка предметов, документов и электронной почтовой корреспонденции, следственного эксперимента, выполняемого с целью опытной проверки показаний.

В оперативно-розыскной деятельности в области расследования компьютерных преступлений целесообразно применять криминологическое прогнозирование индивидуального и преступного группового поведения. Определенную информацию можно извлечь, анализируя сетевой трафик локальных и региональных компьютерных сетей. Полезную информацию могут дать и анализ платежей клиентов за телефонные услуги.

Прогнозирование может успешно осуществляться в основе первичных материалов оперативного учета, так как его банки информации создаются на основе прогноза вероятности преступного поведения определенных криминогенных контингентов. Именно прошлое их поведение (суди-

мость, правонарушения, антиобщественные поступки, большие успехи в области программирования), настоящее (поддержание криминальных связей, паразитизм, склонность к антиобщественным занятиям, склонность создавать программы «вандалы») дают основания для прогностических выводов о вероятном противоправном поведении в будущем.

Принимаются во внимание социальные оценки, даваемые лицу, представляющему оперативный интерес, роль для него мнения представителей криминогенной и преступной среды. Все это в совокупности является элементами методики криминологического прогнозирования, которое вплетается в оперативно-розыскные мероприятия при реализации форм оперативно-розыскной деятельности (далее – ОРД) (поиске, профилактике, разработке). Естественно, вопросы моделирования и прогнозирования необходимо решать, используя современные информационные технологии в процессе информационно-аналитической деятельности.

Информационно-аналитическая деятельность в сфере борьбы с организованными формами преступной деятельности является составной частью процесса обеспечения государственной системы противодействия преступности в целом.

Следует отметить, что решение задач поиска, отбора и систематизации такого рода информации предполагает использование интегрированной информационной системы, возможности которой позволяют существенно расширить информационную базу, необходимую для информационно-аналитического обеспечения, снизить затраты времени на поиск и отбор исходной информации, своевременно определять аспекты, по которым следует проводить анализ информации, а главное – в процессе аналитической обработки данных обеспечить выявление сущности и динамики пространственно-временных и причинно-следственных связей между исследуемыми фактами, явлениями, процессами.

В результате первоначально имеющиеся данные преобразуются в новую, выводную информацию, которая позволяет готовить предложения по нейтрализации криминальных угроз, принимать обоснованные оперативные и управленческие решения, подготавливать планы действий, правильно распределять силы и средства, осуществлять координацию и взаимодействие.

Таким образом, информационно-аналитическое обеспечение деятельности правоохранительных органов по линии борьбы с преступной деятельностью представляет собой систему, включающую в себя два взаимосвязанных компонента.

1. Первый – это информационное обеспечение, которое состоит в изучении информационного спроса потребителей, поддержании устойчивого состояния информационных связей, сборе, накоплении, обработке, хранении и выдаче информации потребителям в максимально короткие сроки.

2. Аналитическое обеспечение, заключающееся в исследовании криминальных угроз, выявлении причин и условий, влияющих на формирование обстановки, прогнозировании ее развития, изучении проблемных ситуаций в сфере противодействия организованной преступности. Конечной целью реализации двух вышеуказанных составляющих информационно-аналитического обеспечения является создание условий для реализации задач уголовной политики государства.

В ряде составов информационных преступлений мотивация поведения преступника имеет особое значение. Преступные мотивы есть по сути своей модификации обычных человеческих мотивов, но направленные на цели, запрещенные законом или связанные с использованием противоправных средств, они являются основополагающими в исправлении и перевоспитании правонарушителей, осуществляемом с помощью методов оперативно-розыскной деятельности.

Такое понимание мотивации преступного поведения исключает представление об обреченности человека на преступное поведение, о неисправимости преступников. В связи с этим для осуществления оперативно-розыскных мероприятий сотрудниками в области информационных технологий определенный интерес представляют социологические и психологические исследования молодежи, обучающейся компьютерным наукам.

Для профилактической деятельности по предотвращению компьютерных преступлений важно проводить изучения мотивов поступков человека. Особый интерес представляет определение уровня ценностно-ориентационного единства в молодежной аудитории (далее – ЦОЕ). По уровню ЦОЕ можно определить факторы, влияющие на поведение человека в группах и в какой-то степени спрогнозировать его стремления к противоправным действиям. Существует методика определения ЦОЕ, которую можно использовать при прогнозировании компьютерной преступности в молодежной аудитории.

Получение любой информации о преступной деятельности требует определенных тактических усилий и организационных форм: действий негласных сотрудников, оперативно-поисковых групп, оперативных контактов с гражданами. И все же многие сведения о традиционных преступлениях (кражи, вывоз похищенных материальных ценностей, владение оружием) по сравнению со сведениями о преступлениях в сфере высоких технологий как будто лежат на поверхности: их можно визуально фиксировать, видеть предметы.

Преступления в области информационных технологий довольно часто можно получить лишь изучением отношений, то есть глубинных явлений, часто никак не фиксируемых визуально и по материальным следам. В качестве примера можно привести факт. Сведения о преступлениях в сфере электронной торговли не принято афишировать коммерческими струк-

турами. Часто они предпочитают понести убыток, чем потерять свою репутацию.

Учитывая, что основным пространством совершения преступления является всемирная сеть Интернет, то процесс сбора оперативной информации можно автоматизировать путем использования специальных программ, называемых интеллектуальными агентами (в среде программистов еще называемых «пауками»). Они способны проводить анализ сайтов, целевой поиск информации в Интернете и тем самым значительно сужать круг поиска подозреваемых.

Сейчас в ОВД России накоплен значительный массив оперативно-розыскной и справочной информации, используемой правоохранительными органами для проведения оперативно-следственных и розыскных мероприятий, а также для решения иных служебных задач. Оперативно-аналитический поиск дает возможность при раскрытии преступлений в сфере высоких технологий использовать компьютерное моделирование. Одним из перспективных направлений компьютерной инженерии является использование имитационных моделей, что предусматривает организацию информационных потоков внутри моделируемых систем, воспроизведение на компьютере операций обмена, перераспределения, взаимодействия между отдельными структурными элементами системы и поэтому является достаточно эффективным средством изучения и прогнозирования преступности.

ГЛАВА 2. ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ НА ОСНОВЕ СОВРЕМЕННЫХ МЕТОДОВ ИНТЕЛЛЕКТУАЛИЗАЦИИ И АВТОМАТИЗАЦИИ

§ 1. Системы управления базами данных в органах внутренних дел

Базы данных являются неотъемлемой составляющей хранилищ данных органов внутренних дел. Классификация информационных баз зависит от того, какое подразделение органов внутренних дел использует базу данных и какие задачи поставлены перед данным подразделением.

На данный момент система управления базами данных продолжает развиваться в сети Интернет для комфортного поиска и получения информации пользователем, начиная от простого поискового запроса, заканчивая разработкой новых баз данных.

Анализ состава информационных ресурсов МВД России позволяет разделить их на шесть групп:

1. Информационные ресурсы управленческого и справочного характера.
2. Оперативно-справочные и розыскные информационные ресурсы.
3. Экспертно-криминалистические информационные ресурсы.
4. Статистические информационные ресурсы.
5. Информационные ресурсы Интерпола и используемые ОВД информационные ресурсы других правоохранительных и иных государственных органов РФ.
6. Информационные ресурсы образовательных учреждений МВД России и системы научно-технической информации.

Первой составляющей информационных ресурсов МВД России являются *информационные ресурсы управленческого и справочного характера*. В деятельности ОВД создается значительное количество нормативных и ненормативных управленческих документов. Документы создаются и пересылаются в «бумажном» и электронном виде. Причем электронный документооборот в последние годы значительно возрос.

Одной их ключевых целей документооборота является создание информационных ресурсов управленческих документов. Для этого в ОВД организовано текущее и архивное хранение документов. После исполнения документы объединяются в дела. Сформированные дела хранятся установленные сроки и используются в деятельности ОВД, а в отдельных случаях в деятельности других правоохранительных и государственных органов.

Основой электронного документооборота в МВД России является положение о системе передачи информации с ограниченным доступом

(далее – СПИОД)[1], не содержащей сведений, составляющих государственную тайну, в технических каналах связи в системе МВД России. Указанное положение устанавливает возможность передачи информации, в том числе заверенной электронной цифровой подписью, через защищенную систему передачи данных, а также регламентирует порядок обмена информацией конфиденциального характера в электронной форме.

Также к информационным ресурсам управленческого и справочного характера относятся следующие информационные ресурсы:

– информационные ресурсы нормативно-правового характера, объединенные в базы данных «Нормативно-правовые акты», «Судебная практика», «Международные договоры», «Юридическая консультация» в рамках СТРАС «Юрист»;

– информационные ресурсы о сотрудниках ОВД, объединенные в базу данных «Кадры», информационные ресурсы штатного расписания;

– информационные ресурсы о финансировании МВД России, объединенные в автоматизированную систему управления.

Второй составляющей информационных ресурсов МВД России являются *оперативно-справочные и розыскные информационные ресурсы*.

Информационные ресурсы оперативно-справочного и розыскного характера создаются в дежурных частях оперативными работниками, участковыми инспекторами полиции, следователями, сотрудниками экспертно-криминалистических и лицензионно-разрешительных подразделений, сотрудниками паспортно-визовых служб и других подразделений. Указанные информационные ресурсы создаются на основе документов первичного учета, в учетных журналах и на других носителях. Они включают в себя сведения о:

– людях, в том числе совершивших преступления и правонарушения;

– предметах, в том числе оружии и автотранспорте;

– помещениях (адресах);

– нераскрытых преступлениях;

– происхождении и принадлежности обнаруженных вещественных доказательств и т. д.

Информация оперативно-справочного и розыскного характера объединяется в информационные ресурсы в информационных центрах МВД России, региональных УМВД, УМВДТ. На федеральном уровне информационные ресурсы оперативно-справочного и розыскного характера

[1] Об утверждении положения о системе передачи информации с ограниченным доступом (СПИОД), не содержащей сведений, составляющих государственную тайну, в технических каналах связи в системе МВД России : приказ МВД России от 7 августа 2004 г. № 497 дсп // Доступ из базы данных «Нормативно-правовые акты МВД России» (дата обращения: 24.01.2022).

концентрируются в Главном информационно-аналитическом центре МВД России.

Внедрение навигационно-мониторинговых систем для позиционирования служебного автотранспорта (с использованием глобальной навигационной спутниковой системы – ГЛОНАСС), а также формирование в муниципальных образованиях элементов аппаратно-программного комплекса «Безопасный город» и введение в эксплуатацию стационарных и удаленных рабочих мест доступа к информационным ресурсам позволит добиться четкого и слаженного взаимодействия нарядов ППС, ДПС ГИБДД, вневедомственной охраны под руководством дежурной части ОВД.

Третьей составляющей информационных ресурсов МВД России являются *информационные ресурсы экспертно-криминалистической направленности*. Для производства экспертиз и исследований правоохранительные органы используют огромное количество разнообразной как чисто криминалистической, так и справочно-вспомогательной информации. Для хранения и использования указанной информации в экспертных учреждениях МВД России созданы экспертные автоматизированные информационные системы и автоматизированные банки данных практически по любому виду экспертиз. Основными информационными ресурсами экспертной информации являются автоматизированные дактилоскопические информационные системы (далее – АДИС) и автоматизированные баллистические идентификационные системы (далее – АБИС).

АДИС применяются при ведении дактилоскопических автоматизированных учетов, в целях осуществления оперативной проверки следов пальцев рук, изымаемых с места происшествия, по массивам дактилокарт ранее осужденных или определенного круга подозреваемых лиц. Информационные ресурсы о дактилоскопических учетах являются одними из основных информационных ресурсов МВД России. Необходимо отметить, что формирование и ведение подавляющего большинства дактилоскопических учетов осуществляет МВД России.

АБИС позволяют идентифицировать оружие по стреляным пулям и гильзам. Посредством АБИС возникла возможность автоматизировать всю технологическую цепочку трасологических исследований пуль, гильз и их фрагментов: от ввода информации и создания электронной базы данных, проверок и сравнительных исследований до получения экспертного заключения.

Также к информационным ресурсам экспертно-криминалистической направленности относятся информационные ресурсы автоматизированных лабораторий ДНК-анализа, лабораторий, занимающихся фоноскопическими исследованиями.

Четвертой составляющей информационных ресурсов МВД России являются *статистические информационные ресурсы* о преступности. В них входит информация о преступлениях, лицах их совершивших, о мате-

риальном ущербе и изъятии предметов преступной деятельности, о потерпевших, о движении уголовных дел и результатах их рассмотрения судом первой инстанции. Статистические информационные ресурсы о преступности в настоящий момент представляют собой единую систему учета преступлений, формирование которой осуществляется разными правоохранительными ведомствами, а ведение и использование поручено МВД России.

Пятой составляющей информационных ресурсов МВД России являются информационные ресурсы Интерпола и используемые ОВД информационные ресурсы других правоохранительных и иных государственных органов РФ. Национальное центральное бюро Интерпола формирует информационные ресурсы о лицах, организациях, событиях, предметах и документах, связанных с преступлениями, носящими международный характер, а также справочно-информационный фонд.

Шестой составляющей информационных ресурсов МВД России являются *информационные ресурсы образовательных учреждений МВД России и системы научно-технической информации*. К информационным ресурсам образовательных учреждений относятся, в частности, фонды библиотек образовательных учреждений. Кроме того, в каждом вузе создан информационный образовательный центр, в котором формируются электронные информационные ресурсы для самостоятельной работы курсантов и слушателей. Информатизация образовательных учреждений МВД России является составной частью информатизации ОВД и включает в себя информатизацию:

– учебно-воспитательного процесса;

– научных исследований;

– служб, обеспечивающих учебный процесс и жизнедеятельность образовательного учреждения;

– процесса координации деятельности образовательных учреждений.

Система научно-технической информации МВД России предназначена для информационного обеспечения оперативно-служебной и иной деятельности органов, подразделений, учреждений внутренних дел, проводимых в МВД России научно-исследовательских и опытно-конструкторских работ, учебного процесса в образовательных и научно-исследовательских учреждениях МВД России на базе информационных ресурсов, накапливаемых в результате обработки сведений о достижениях науки и техники, положительного опыта деятельности ОВД РФ и зарубежных правоохранительных органов.

Информационные ресурсы системы научно-технической информации МВД России (далее – СНТИ) содержат материалы об опыте работы ОВД России, деятельности правоохранительных органов зарубежных стран, а также сведения о результатах проводимых в системе МВД России научно-исследовательских и опытно-конструкторских работ и диссертационных исследований.

§ 2. Автоматизация системы управления в органах внутренних дел

Эффективность борьбы с преступностью определяется уровнем организации оперативной, следственной, профилактической работы, проводимой ОВД. В свою очередь, результаты этой работы зависят от качества информационной поддержки, поскольку основные усилия практических работников в расследовании, раскрытии и предотвращении преступлений так или иначе связаны с получением необходимой информации, именно эти функции и призвана обеспечить система информационного обеспечения ОВД, которая поддерживает в настоящее время значительный объем информации.

Интегрированные банки данных МВД России служат для автоматизации бизнес-процессов служебной деятельности сотрудников подразделений МВД России на федеральном и региональном уровнях при формировании, ведении и использовании централизованных оперативно-справочных, разыскных и криминалистических учетов.

Интегрированные банки данных представляют основной вид информационного обеспечения оперативно-служебной деятельности сотрудников ОВД с 1993 года, находясь в постоянном развитии.

В настоящее время в ФКУ «ГИАЦ МВД России» и информационных центрах территориальных органов МВД России эксплуатируются программно-технические комплексы интегрированных банков данных (далее – ИБД) общего пользования федерального (ИБД-Ф) и регионального (ИБД-Р) уровней.

Интегрированные банки данных (ИБД-Ф и ИБД-Р) находятся в тесном информационном взаимодействии. Помимо этого они предоставляют для других информационных систем сервис ввода информации с ее дальнейшей интеграцией и поисковые возможности.

В состав программного обеспечения ИБД входят:

– база данных системы с интегрируемыми элементами;

– рабочие места пользователей в виде почтовых и веб-клиентов;

– подсистемы, специализированные по направлениям деятельности МВД России;

– подсистема генерации отчетов;

– сервисы обеспечения взаимодействия с системой межведомственного взаимодействия для обеспечения выполнения государственных услуг в электронном виде.

Автоматизация лишь отдельных процессов деятельности МВД России привела к ситуации, когда информационные массивы служб и подразделений ОВД оказались слабо интегрированы между собой, что крайне затрудняло решение задач, стоящих перед МВД России, таких как:

– борьба с межрегиональными и серийными квалифицированными преступлениями;

– работа с преступлениями, которые не раскрыты, посредством поиска типичных преступлений и идентификации лиц;

– подготовка аналитической и сводной статистической информации по формированию и ведению централизованных оперативно-справочных, разыскных и криминалистических учетов.

Для решения описанных выше задач было принято решение разработать программное обеспечение интегрированного банка данных федерального уровня (ИБД-Ф), формируемого на основе данных из различных автоматизированных систем департаментов и управлений МВД России, подразделений территориальных органов МВД России, федеральных органов исполнительной власти.

В настоящий момент ИБД-Ф включает в себя следующие подсистемы, обеспечивающие формирование и ведение централизованных учетов:

– «Картотеку» – оперативно-справочный (пофамильный) учет;

– «АБД-Центр» – учет преступлений и лиц, подозреваемых, обвиняемых в их совершении;

– «Номерные вещи» – учет похищенных и изъятых номерных вещей и документов;

– «ФР-Оповещение» – учет лиц, объявленных в федеральный и межгосударственный розыск;

– «Оружие» – учет утраченного или выявленного огнестрельного оружия и иного вооружения;

– «Автопоиск» – учет разыскиваемых транспортных средств и информационное взаимодействие с автоматизированной системой оперативного информирования ОВД Российской Федерации о похищенных автомототранспортных средствах, состоящих на учете в Генеральном секретариате Интерпола и т. д.

В ходе деятельности территориальные органы МВД России оперируют значительными объемами информации по различным объектам учета, находящимся в сфере их интересов. Возникает задача оперативной регистрации, распространения, обработки и хранения этой информации.

В связи со значительной унифицированностью процессов во всех территориальных органах МВД России возможна разработка типового решения.

На региональном уровне ИБД-Р обеспечивает взаимодействие с основными информационными системами для обеспечения сотрудников полиции необходимой информацией.

В качестве типового программного обеспечения было разработано унифицированное прикладное математическое обеспечение (УПМО) ИБД-Р, имеющее в своем составе следующие программные комплексы (рис. 2):

– «Интегрированный банк данных» (ИБД), на базе которого осуществляется формирование и ведение разыскных, криминалистических и

профилактических учетов территориальных органов МВД России. В ИБД собирается и хранится общая информация об объектах учета, информация о связях объектов учета с учетными документами;

– «Оперативно-справочная картотека» (ОСК), обеспечивающая формирование в территориальных органах МВД России автоматизированного оперативно-справочного учета (пофамильной картотеки) лиц, подозреваемых или обвиняемых в совершении преступления, осужденных за совершение преступлений;

– «Автоматизированная информационно-справочная система «Статистика» (АИСС «Статистика»), обеспечивающая учет и обработку документов первичного учета статистических карточек и формирование на их основе государственной статистической отчетности о преступности в территориальных органах МВД России;

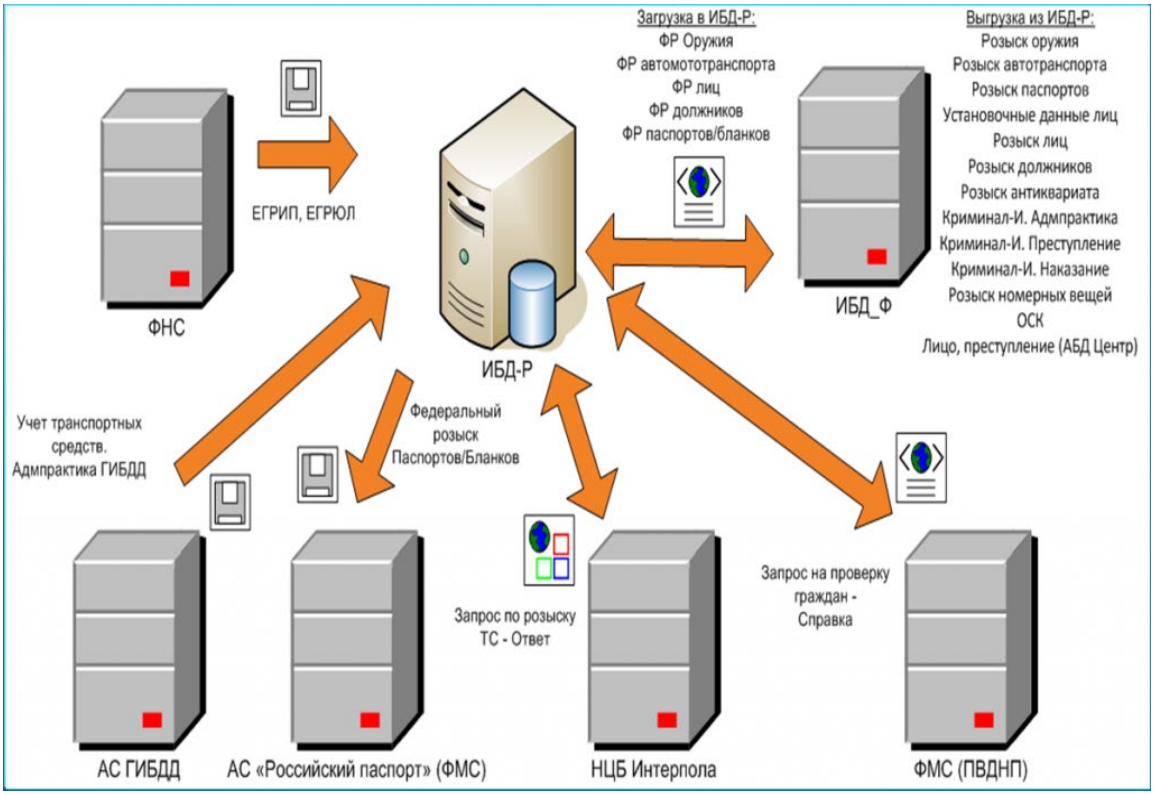

Рис 2. Контур банка данных регионального уровня и взаимодействие с основными информационными системами для обеспечения сотрудников полиции необходимой информацией

– «МОСТ Р Регион» – программный комплекс, позволяющий получать и формировать на основе унифицированных отчетных срезов нерегламентные статистические отчеты по заданиям сотрудников Центрального аппарата МВД России, формируемые в ПК «МОСТ Р» федерального уровня.

Таким образом, программно-технические комплексы МВД России являются одним из ключевых компонентов повышения эффективности информационного обеспечения в ОВД и позволяют:

– интегрировать разрозненные информационные ресурсы ОВД в единый банк данных;

– организовать эффективное информационное взаимодействие информационных систем ОВД;

– обеспечить оперативный и безопасный доступ сотрудников ОВД к интегрированному банку данных, в том числе в режиме удаленного доступа.

В настоящее время в сервисе управления доступом к информационным ресурсам и системам ИСОД МВД России имеется около 350 000 учетных записей пользователей, разработано порядка 40 прикладных сервисов, что является показателем востребованности системы, являющейся ключевым элементом информационного обеспечения в повышении эффективности управления.

§ 3. Единая информационно-телекоммуникационная инфраструктура МВД России

Одним их наиболее актуальных направлений совершенствования информационного обеспечения управления в ОВД является использование информационных технологий в деятельности сотрудников, а также формирование единой актуальной базы данных оперативно-служебной деятельности.

Использование информационных технологий предполагает реализацию межведомственного взаимодействия, данных, размещенных в телекоммуникационных системах, сети Интернет. В настоящее время использование информационных технологий в решении оперативных задач набирает все большую популярность, а в некоторых областях, например, в области компьютерной криминалистики, является их неотъемлемой частью. Это открывает новые горизонты и способствует повышению уровня эффективности управления.

Основными критериями эффективности использования информационных технологий в информационном обеспечении служебной деятельности являются:

– использование современных информационных технологий, программного и аппаратного обеспечения;

– подготовка квалифицированных кадров;

– долгосрочный характер развития и использования информационных систем;

– общая техническая оснащенность.

Совершенствование информационных систем должно быть направлено на ликвидацию задержек поступления и обработки информации; фактов ее избытка, несопоставимости сообщений, дублирования данных; низкого коэффициента использования информации. В современных условиях, открывающих возможность использования достижений научно-технического прогресса, первоочередной задачей в рассматриваемой сфере деятельности становится создание на базе ЭВМ и других технических средств современной единой информационно-телекоммуникационной системы.

Так, в 2004 году была образована Дирекция Программы МВД России, а уже к концу года была утверждена сама Программа МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел», целью которой являлось повышение эффективности деятельности ОВД, обеспечение законности, правопорядка и общественной безопасности путем совершенствования информационного обеспечения на основе реконструкции и оборудования объектов ОВД новыми и перспективными телекоммуникационными и программно-техническими комплексами с использованием современных телекоммуникационных, информационных и биометрических технологий.

В 2012 году МВД России утвердило новую концепцию создания единой системы информационно-аналитического обеспечения деятельности (далее – ИСОД) МВД России, которая заключалась в комплексном использовании в министерстве новейших информационных систем, телекоммуникационного оборудования, программно-аппаратных комплексов и систем связи, что являлось крайне необходимым условием качественного обеспечения служебной деятельности.

Разработка системы ИСОД МВД России стала продолжением проекта развития единой информационно-телекоммуникационной системы ведомства.

Разрабатываемая система должна была так же решить проблему отсутствия единого подхода к использованию архитектурных решений и комплексного подхода к внедрению информационных систем в ОВД, использованию банка данных для решения оперативных задач.

В настоящее время деятельность ОВД немыслима без использования современных телекоммуникационных технологий, позволяющих обеспечить оперативный обмен информацией и эффективное взаимодействие различных подразделений МВД России. Именно эти обстоятельства обусловили потребность в создании единой информационно-телекоммуникационной системы ОВД.

Введение в эксплуатацию системы ИСОД МВД России было осуществлено в 2015 году. На тот момент к интегрированной мультисервисной системе было подключено порядка 25 000 автоматизированных рабочих мест.

Планово проводятся мероприятия по увеличению мощностей центра обработки данной системы, совершенствованию коммуникационного оборудования и технических средств, реорганизации и повышению пропускной способности каналов связи. В круглосуточном режиме осуществляется техническая поддержка пользователей ИСОД МВД России, что способствует эффективному информационному обмену данными.

Отдельным аспектом является повышение уровня информационной безопасности системы, для чего был разработан комплекс организационно-технических мер по повышению культуры информационной безопасности при работе в системе, в том числе реализована масштабная антивирусная инфраструктура.

Основными структурными компонентами ИСОД МВД России являются: Центр обработки данных, интегрированная телекоммуникационная сеть, сервисы обеспечения повседневной служебной деятельности сотрудников ОВД, системы межведомственного взаимодействия и подсистема обеспечения информационной безопасности.

Прикладные сервисы обеспечения деятельности сотрудников ОВД представлены следующим перечнем:

– сервис электронного документооборота;

– сервис электронной почты;

– ведомственный информационно-справочный портал;

– система видео-конференц-связи.

Прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД России на сегодняшний день представлены следующим перечнем (рис. 3):

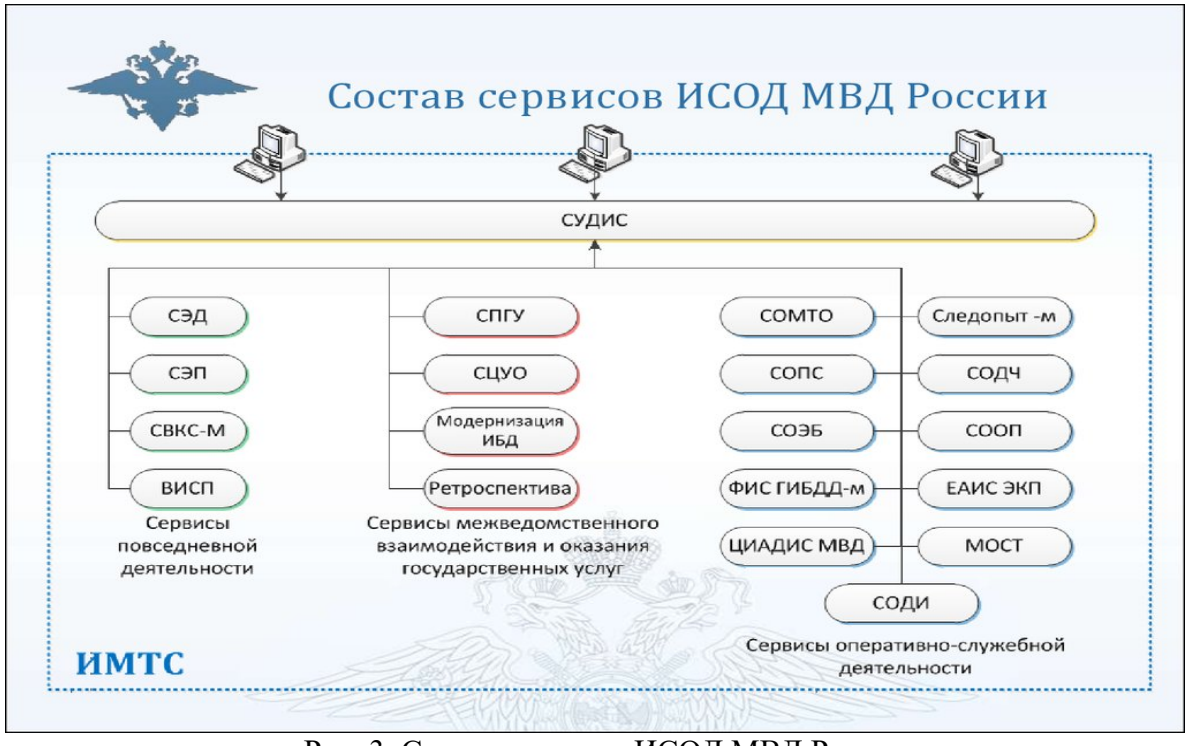

Рис. 3. Состав сервисов ИСОД МВД России

Сервис управления доступом к информационным системам (далее – СУДИС) является одним из ключевых элементов подсистемы информационной безопасности ИСОД МВД России. Он обеспечивает:

– управление доступом пользователей в систему;

– управление доступом пользователей к сервисам ИСОД МВД России;

– единую точку входа в сервисы ИСОД МВД России;

– регистрацию событий безопасности.

СУДИС позволяет:

– организовать контроль пользователей, имеющих доступ к сервисам ИСОД;

– обеспечить доступ к ресурсам по электронной подписи.

На каждом автоматизированном рабочем месте (далее – АРМ) сотрудника МВД России, входящем в состав ИСОД МВД России и (или) подключенном к интегрированной мультисервисной телекоммуникационной сети (ИМТС), должны быть установлены и использоваться следующие средства защиты информации:

1. СУДИС МВД России. Вход в операционную систему, установленную на АРМ, должен осуществляться исключительно посредством программного обеспечения СУДИС.

2. ViPNet Client . Установка ViPNet Client на АРМ должна выполняться вне зависимости от количества аппаратных комплексов ViPNet Coordinator. ViPNet Client должен быть настроен на работу во 2-м режиме средствами центра управления ViPNet-сетью.

3. Антивирус Касперского.

4. Агент антивируса Касперского. Агент должен быть подключен к серверу администрирования Kaspersky Security Center ИСОД МВД России.

5. КриптоПро CSP.

6. Драйвер Рутокен.

Вместе с тем сотрудником МВД России, работающим на АРМ, должен быть получен ключевой носитель Рутокен с записанным на него ключом электронной подписи, привязанным к персональной учетной записи СУДИС сотрудника МВД России.

Функциональные задачи СУДИС:

1. Управление доступом пользователей в операционную систему.

2. Управление доступом пользователей к сервисам ИСОД МВД России.

3. Управление доступом сервисов ИСОД МВД России к другим сервисам ИСОД МВД России.

4. Единая точка входа в сервисы ИСОД МВД России.

5. Регистрация событий безопасности.

6. Управление полномочиями пользователей ИСОД МВД России.

7. Обеспечение доступа к ресурсам ИСОД МВД России с использованием электронной подписи.

В каждом территориальном подразделении МВД России регионального уровня назначается уполномоченное лицо, ответственное за создание учётных записей (далее – УЗ) пользователей – администратор доступа. Количество и зона ответственности администраторов доступа определяются в каждом территориальном подразделении МВД России самостоятельно.

Назначение производится приказом «О назначении уполномоченных лиц, ответственных за процесс создания, изменения, блокирования учётных записей пользователей ИСОД МВД России в подразделениях системы МВД России». Копия приказа в электронном виде должна быть направлена в адрес единого центра эксплуатации ИСОД МВД России (далее – ЕЦЭ) (по электронной почте либо по факсу на единый номер поддержки). Оператор ЕЦЭ регистрирует обращение. В срок не более пяти рабочих дней выполняется создание учётной записи администратора доступа. Администратор доступа может уточнить статус обработки обращения через оператора ЕЦЭ.

Логин и временный пароль администратору доступа сообщаются по указанному в приказе телефону сотрудником ЕЦЭ.

В обязанности администратора доступа входит:

– сбор сведений об организационной структуре подразделений, в которых производится внедрение и эксплуатация сервисов ИСОД;

– формирование и отправка заявок на создание УЗ пользователей;

– получение логинов и временных паролей пользователей и их выдача сотрудникам подразделения;

– ответственность за полноту и достоверность предоставленных сведений.

Учётная запись пользователя должна отражать актуальную информацию о пользователе. Пользователь несёт ответственность за достоверность предоставленных сведений и своевременное информирование администратора доступа о произошедших изменениях в личной и служебной информации согласно полям формы заявки.

По запросу пользователя администратор доступа оформляет заявку на изменение учётных записей с указанием следующих данных: логина, ФИО, подразделения, должности, вносимых изменений, оснований внесения изменений. Заполненную по форме заявку администратор доступа должен выслать со своего персонального служебного почтового адреса на адрес ЕЦЭ. Оператор ЕЦЭ регистрирует обращение и сообщает уникальный идентификатор заявки. В срок не более 5-ти рабочих дней выполняется изменение учётных записей пользователей. Администратор доступа может уточнить статус обработки обращения через оператора ЕЦЭ по единому телефону поддержки.

В результате обработки заявки на изменение учётных записей пользователей администратору доступа на персональный служебный почтовый адрес поступает информация об изменении. Блокирование учётных записей пользователя осуществляется при увольнении сотрудника, при получении информации о компрометации (или при подозрении на компрометацию) его УЗ и в иных случаях по решению непосредственного руководителя сотрудника. Разблокирование УЗ производится по решению непосредственного руководителя соответствующего сотрудника.

Руководитель подразделения направляет администратору доступа логин, ФИО пользователя, для которого производится блокирование или разблокирование УЗ. По запросу руководителя подразделения администратор доступа оформляет заявку на блокирование или разблокирование учётных записей с указанием следующих данных: логина, ФИО, подразделения пользователя. Заполненную в свободной форме заявку администратор доступа должен выслать со своего персонального служебного почтового адреса на адрес ЕЦЭ. Оператор ЕЦЭ регистрирует обращение и сообщает уникальный идентификатор заявки. В срок не более одного рабочего дня выполняется блокирование или разблокирование УЗ пользователя. В результате обработки заявки администратору доступа на персональный служебный почтовый адрес поступает подтверждение о произведённом блокировании или разблокировании.

В настоящее время деятельность ОВД немыслима без использования современных телекоммуникационных технологий, позволяющих обеспечить оперативный обмен информацией и эффективное взаимодействие различных подразделений МВД России.

§ 4. Экономическая основа компьютерных преступлений и борьба с ними в сфере правоохранительной деятельности

Основными методами информационно-аналитической работы подразделений экономической безопасности и противодействия коррупции (далее – ЭБиПК) являются сканирование обрабатываемой информации и интеграция всех сведений, касающихся изучаемого объекта. При этом очевидно, что наиболее перспективной возможностью повышения эффективности управления процессами противодействия экономическим преступлениям в настоящее время является применение информационных технологий.

Известно, что признаки всевозможных угроз и правонарушений проявляются в разное время и со стороны различных объектов, фиксируются с различной степенью полноты и детализации различными источниками. В связи с этим установление причинно-следственной связи между происхо-

дящими событиями и возможными преступлениями требует проведения многофакторного анализа собранной информации.

Анализ информации и ее синтез позволяют выявить криминальные устремления к предприятию со стороны организаций и физических лиц, связанных с криминальными структурами, распознать негативные тенденции в перераспределении акций (приобретение монопольного влияния на предприятие со стороны «портфельных спекулянтов», иных недобросовестных партнеров), предотвратить криминальные устремления к акционерам из числа руководителей и сотрудников предприятия, собрать необходимые материалы для заведения уголовного дела. Всю эту работу быстро и эффективно можно осуществлять с помощью автоматизированных систем информационно-аналитической поддержки.

В настоящее время разработаны и успешно эксплуатируются интегрированные банки данных, где модель предметной области позволяет организовать слияние разнородных сведений по одним и тем же объектам (лицам, фирмам, адресам, телефонам, автотранспортным средствам). Таким образом, при введении новых объектов происходит установление связей между ними и уже имевшимися объектами, а также дополнение уже имевшихся объектов новыми характеристиками. В результате наращивается сетевая структура связей объектов и образуется информация, не вводившаяся в явном виде в банк данных. Подобная структура предметной области интегрированных банков данных позволяет от одного информационного объекта выйти на все его окружение.

Информация из интегрированных банков данных позволяет решать как учетно-справочные и статистические задачи (кадры, контакты, события, партнеры, конкуренты, реклама и др.), так и информационно-логические задачи (экспресс-оценка хозяйствующего субъекта, оценка угрозообразующих факторов и угроз, анализ подозрительных с криминальной точки зрения событий, изучение сомнительных связей объекта, оценка сфер влияния, конфликтных и кризисных ситуаций и т. д.). При этом используются информационные ресурсы как внутренних, так и внешних по отношению к ОВД баз данных различных уровней (федеральный, региональный, ведомственный и локальный).

Информационно-аналитическое обеспечение в ходе расследования экономических преступлений должно осуществляться следующим образом. Сначала собирается первичная информация, которая может быть получена: оперативным путем, в ходе следствия, документальной проверки или экспертизы, из любой другой организации, из заявлений граждан. Первичная информация также может быть собрана на основе сканирования общедоступных и ведомственных информационных баз данных, где аналитик может обнаружить негативные, криминально опасные тенденции в деятельности интересующего объекта.

Следует отметить, что в современных условиях получение первичной информации оперативным путем значительно сложнее, чем получение ее из открытых источников. Для более глубокого понимания всех скрытых нюансов работы с открытыми источниками информации следует иметь в виду, что в прежние годы правоохранительные органы делали упор на добывание нужной документальной информации. В тот период не было особых трудностей, так как на государственных предприятиях (а их было большинство) администрация и общественные организации активно шли на сотрудничество с правоохранительными органами. Аналогично вели себя и рядовые работники предприятий, основная масса которых искренне «болела» за обеспечение порядка на предприятиях, которые воспринимались как общенародная собственность. В то же время отношение к источникам открытой информации, особенно к периодически изданиям, было как к средствам идеологической пропаганды. Критические, «острые» материалы в газетах и журналах служили поводом для наведения порядка административным путем или назидательным примером руководителям всех уровней и гражданам, склонным к отклоняющемуся поведению.

Совершенно иная обстановка складывается в настоящее время. Правоохранительные органы зачастую не располагают обширными возможностями для получения агентурной информации на частных предприятиях, а администрация этих предприятий и их службы безопасности не заинтересованы раскрывать такого рода данные. В связи с этим самым доступным методом получения оперативной информации сегодня является сбор и обобщение открытых информационных источников. Проделать это можно с использованием IT-технологий, которые позволяют быстро произвести сбор и сопоставить нужную информацию. Сюда входят различные СМИ-источники, сеть Интернет, телефонные справочники, научные журналы, правительственные отчеты, техническая документация, руководства, инструкции, научные и технические обзоры, а также личная информация из социальных сетей. Все это объединяется терминами «OSINT»[1] – это специфическая информация, собранная и особым образом структурированная ради ответа на конкретный вопрос.

Большой опыт в этом отношении накоплен в США. В соответствующих американских учебных пособиях и наставлениях отмечается, что аналитическая работа, базирующаяся на открытых источниках, может привести к важным результатам, которые в некоторых случаях будут значительно превосходить данные, полученные оперативным путем, а также давать возможность делать актуальные выводы и прогнозы.

Далее информационно-аналитическое обеспечение в ходе расследования экономических преступлений должно быть направлено на оценку

[1] Берд К. Модель OSINT // Компьютерра. – 2007. – 6 декабря. – URL : http://old.computerra.ru/think/kiwi/324966/ (дата обращения: 12.01.2022).

собранной информации, которая обязательно должна включать в себя установку достоверности информации. При этом используются учетно-регистрационные данные и другая информация, которая позволяют установить, действительно ли существуют лица и организации, указанные в сообщении, фактическое состояние контролируемого объекта и т. п.

Если первичная информация получена из Интернета, то проверка достоверности информации должна быть обязательным элементом информационно-аналитической работы.

Дело в том, что сегодня в Интернете различные вбросы (слухи, сплетни, домыслы) или, как их нередко называют – фейки, расходятся гораздо быстрее, чем правдивая информация. Следовательно, например, какое-нибудь фото, заинтересовавшее оперативного работника и полученное из блогов или со страниц электронных СМИ, вполне может оказаться результатом чей-то кропотливой работы в Adobe Photoshop и никак не быть связано с реальными событиями. Для определения достоверности информации, полученной в Интернете, можно воспользоваться специальными методами верификации полученных данных, применяя определенные онлайн-инструменты[1].

В информационно-аналитическом обеспечении оперативно-разыскной деятельности может сложиться противоположная ситуация – полученная из общедоступных источников информация заблокирована таким образом, что невозможно определить ее первоисточник или ее авторов. Обычно система работает так: компьютер посылает запрос на сервер вызываемого сайта и оставляет там свои данные в виде уникального IP-адреса. Таким образом, все действия пользователей в том или ином виде сохраняются на серверах интернет-страниц, куда они когда-нибудь заходили, поэтому по IP-адресу компьютера правоохранительные органы практически всегда могут определить реального пользователя и его действия.

Однако в последние годы среди пользователей сети Интернет получили распространение так называемые анонимайзеры. Это специальные сайты, компьютерные программы и приложения, с помощью которых пользователь может скрыть информацию о том, какие страницы и в какое время он посещает, а также что он с них скачивает и чем делится с другими пользователями. Для этого ему достаточно установить на свой компьютер специальное приложение, которое после установки полностью шифрует всю активность хозяина компьютера в Интернете. Тех же результатов можно достигнуть, если подключиться к анонимным сетям. Большинство

[1] И еще раз о фейках : 8 онлайн-инструментов для верификации контента. – URL: http://ain.ua/2014/02/05/511747 (дата обращения: 13.01.2022).

подобных сетей децентрализовано и простым поиском через поисковики страницы анонимных сетей найти невозможно.

Сегодня в анонимных сетях собираются не только любители нелегального скачивания музыки и видеоконтента. Там себя комфортно ощущают всевозможные международные мошенники, торговцы наркотиками и оружием, лица, занимающиеся изготовлением и торговлей детской порнографии, и т. п. Представителей криминального мира в анонимных сетях привлекает относительная безнаказанность и защищенность, тем более что за нелегальные услуги здесь можно заплатить не только традиционным образом, но и с помощью цифровой валюты.

В связи с этим анонимайзеры в последнее время стали объектом повышенного интереса со стороны правоохранительных органов. В оперативно-розыскной деятельности могут использоваться более простые, но эффективные методы. Так, для задержания преступников британская полиция использовала простую рассылку электронных писем на электронные адреса скрывающихся преступников. В письмах им предлагалось в рамках рекламной акции получить ящик бесплатного пива, для чего требовалось позвонить по номеру якобы маркетинговой компании. Преступники называли время и место, где им удобнее всего было бы забрать спиртные напитки, куда с целью ареста выезжал наряд полицейских.

Следующий шаг в информационно-аналитической работе – построение различных оперативных версий и составление плана оперативных мероприятий по дополнительному получению недостающей информации.

Далее осуществляется проверка версий посредством получения, анализа и оценки информации из различных источников (сообщений, внутренних баз данных, внешних информационных массивов, получаемых официально и оперативным путем).

В то же время необходимо учитывать, что информационно- аналитический поиск фактов и признаков правонарушений является только первым шагом на пути выявления и раскрытия преступлений – указанием на субъекта хозяйствования или на конкретное физическое лицо, которые целесообразно взять на оперативную проверку.

Приведем несколько примеров проведения информационно- аналитического поиска фактов и признаков экономических преступлений.

Известно, что сегодня в стране существует огромное количество фиктивных организаций. Они создаются для ведения незаконного бизнеса и ухода от налогов крупными компаниями, для получения доходов путем совершения мошеннических хозяйственных операций и т. д. Наличие фиктивной организации или какие-либо контакты с фиктивной организацией является признаком как минимум нарушения установленного порядка ведения предпринимательской деятельности, а чаще возможных преступлений.

Для того чтобы выявить фиктивное предприятие, можно проверить его на основе специальной методики «109 признаков фирм-однодневок»[1]. Эта методика представляет собой перечень признаков фиктивных организаций и рекомендуемых действий должностным лицам в той или иной ситуации. Следует обратить внимание, что если организация отвечает хотя бы одному из 109 признаков «неблагонадежной фирмы», то она (по документу) должна заноситься в специальный реестр неблагонадежных организаций и подвергнуться специальной оперативно-розыскной разработке.

В данной методике все признаки делятся на три группы:

– признаки, выявляемые на этапе регистрации компании;

– признаки, выявляемые на этапе постановки компании на налоговый учет;

– признаки, выявляемые в ходе деятельности компании.

К сожалению, в этой методике не указан вес (значимость) признаков, что негативно сказывается на объективности оценки компаний. Например, совершенно очевидно, что признак регистрации компании в форме ООО и признак регистрации компании по поддельным документам обладают разной значимостью. В таких случаях аналитику предоставляется возможность самостоятельно ранжировать признаки, исходя из особенностей контролируемого объекта. Следует учитывать, что приоритет признаков может варьироваться в зависимости от целей анализа, отраслевой принадлежности объекта анализа и т. п.

Другим примером является анализ базы данных грузовых таможенных деклараций таможенного комитета России и базы данных регистрационных сведений средств автотранспорта и их владельцев.

Этот анализ позволяет, например, устанавливать юридических и физических лиц, осуществляющих ввоз из стран дальнего и ближнего зарубежья автотранспортных средств, устанавливать налогоплательщиков, активно занимающихся перепродажей автотранспортных средств и т. п.

Однако только анализ различных информационных баз данных, как правило, не позволяет с полной вероятностью выявить совершаемые преступления. Для этого необходима тесная совместная работа аналитиков, управленцев и оперативников.

Последовательность работы по выявлению экономических преступлений должна содержать как сравнение информационных баз данных, так и проведение оперативно-розыскных мероприятий. Наряду с перечисленными выше источниками информации могут использоваться нетрадиционные источники, получаемые оперативным путем. Например: бухгалтерская база данных налогоплательщика; базы данных деловых партнеров и за-

[1] Вопросы Министерства внутренних дел Российской Федерации : указ Президента РФ от 1 марта 2011 г. № 248 // Собрание законодательства РФ. – 2011. – № 10. – Ст. 1334.

ключенных ими контрактов; базы данных коммерческих банков, страховых компаний и др.

Как следует из приведенных выше примеров, очень трудоемким этапом информационно-аналитической работы является сочетание банков данных в смежных областях, содержащих различную отчетную и специальную информацию, а также признаки нарушения законодательства. Сегодня различные ведомства и корпорации уже владеют технологиями, которые позволяют быстро и без участия человека осуществлять эту работу и выдавать специалисту готовые управленческие решения, а также результаты сопоставления различных информационных ресурсов по заранее заданному критерию.

§ 5. Повышение эффективности управления в органах внутренних дел на основе современных методов интеллектуализации и автоматизации в области противодействия кибертерроризму

Поскольку важной составляющей системы управления в ОВД является организация деятельности территориальных органов МВД России по контролю (надзору) за соблюдением отдельными категориями лиц установленных в соответствии с федеральным законом запретов и ограничений, а также осуществлением профилактической работы с населением, целесообразно рассмотреть возможности применения современных методов интеллектуализации и автоматизации с целью повышения эффективности управления на примере области противодействия кибертерроризму.

На сегодняшний день неотложной задачей в области обеспечения информационной безопасности является установление сотрудничества в области противодействия информационному терроризму, поскольку возрастающий уровень преступлений экстремистского и террористического характера, в частности с использованием глобальной сети Интернет, в наши дни является довольно актуальной проблемой, чему способствует всеобщая тенденция по цифровизации общества, активность граждан в сети Интернет, в том числе в социальных сетях, зачастую посредством которых запрещенные организации осуществляют вербовку, пропагандируя запрещенные идеологии[1].

Насущный характер данной проблемы подтверждается статистикой зарегистрированных правоохранительными органами преступлений экс-

[1] Харисова З. И., Сайнеев В. Е. Отдельные аспекты противодействия экстремизму и терроризму в сети Интернет // Идеалы и ценности ислама в образовательном пространстве XXI века : материалы Международной научно-практической конференции, приуроченной к 30-летию открытия первого в постсоветском пространстве мусульманского медресе при ЦДУМ России имени Ризаэтдина бинэ Фахретдина (23 октября 2019 г.) Уфа : Печать, 2019. С. 367–370.

тремистского и террористического характера, а особенно их низкий уровень раскрываемости. Отчасти виной тому является массовое внедрение и использование инфокоммуникационных технологий.

Статистика зарегистрированных правоохранительными органами Российской Федерации за 2010–2020 годы лиц[1], совершивших преступления террористического характера, например, по сравнению с 2016 годом характеризуется тенденцией к снижению уровня преступности (рис. 4), однако только за последний год раскрываемость преступлений такого рода снизилась на 25 %.

Статистика зарегистрированных правоохранительными органами Российской Федерации за 2010–2020 годы лиц, совершивших преступления экстремистского характера, в целом благоприятна (рис. 5), однако раскрываемость их снизилась на 2 %.

Данная статистика негласно подтверждает тот факт, что растет профессионализм злоумышленников, а это в большей мере обусловлено применением тех или иных инфокоммуникационных технических решений.

Наращиванию агрессивных, экстремистских, преступных тенденций в обществе способствуют средства массовой информации, сеть Интернет и социальные сети, зачастую посредством которых экстремистские и террористические организации осуществляют вербовку молодых людей в свои группировки, пропагандируя разрушительные идеи. Кроме того, важным аспектом является обеспечение «социального» здоровья людей, которое включает в себя не только физическое, психическое и духовное благополучие, но и «здоровую» гражданскую позицию.

Открытым на сегодняшний день остается вопрос о профилактическом воздействии средств массовой информации, сети Интернет и социальных сетей на молодежную среду общества для дальнейшей возможности предотвращения вербовки и пропагандирования запрещенных идей. Если раньше экстремисты достигали своих целей путем силового давления, то в настоящее время их характерной чертой является активное вовлечение в данный процесс технических методов и средств, т. е. вместо обычных насильственных мер применяется информационное управление мышлением.

[1] Сборник о состоянии преступности в России (2010–2020 гг.) // Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации. – URL : http://crimestat.ru/analytics (дата обращения: 16.01.2022).

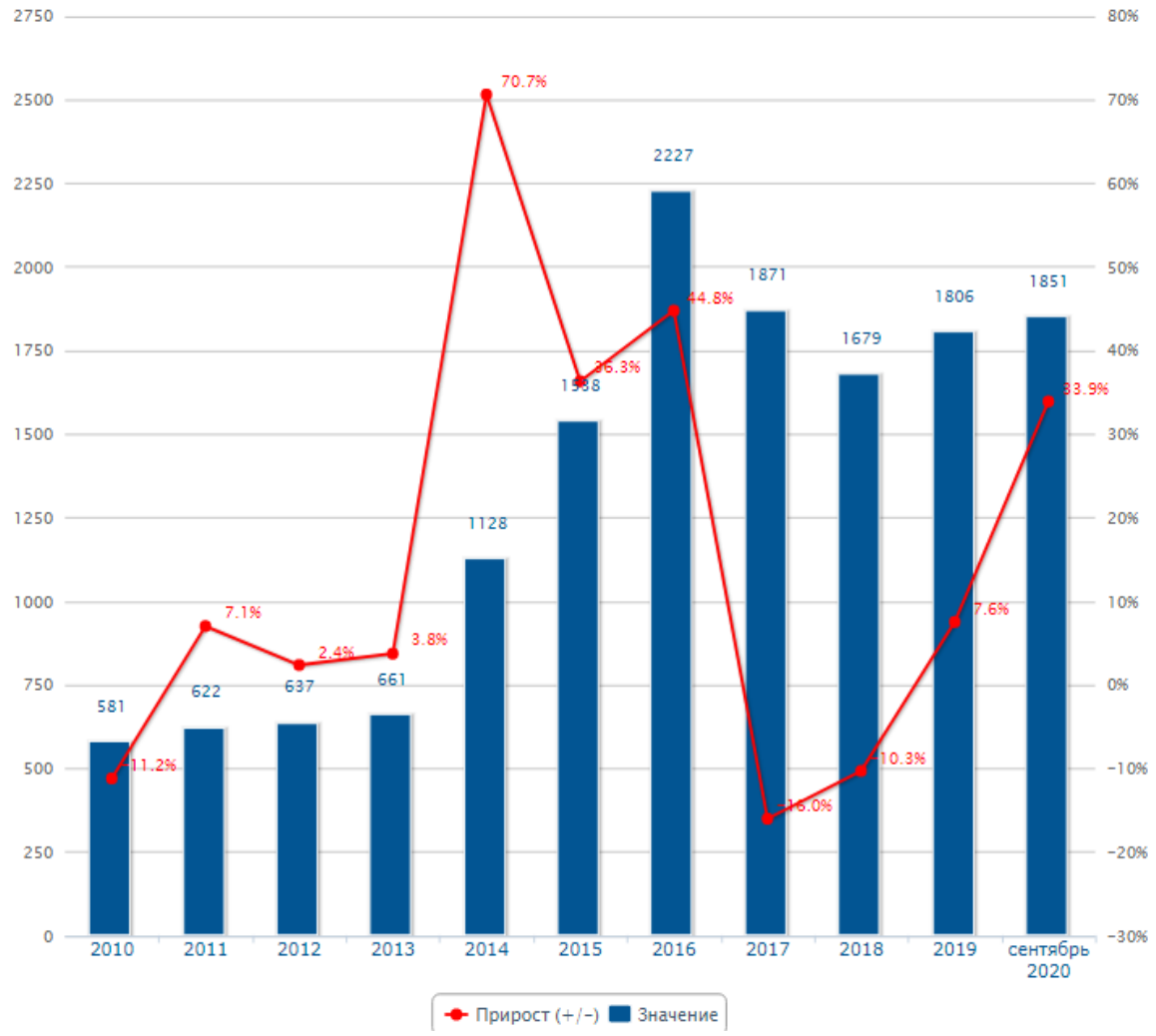

Рис. 4. Зарегистрированные за 2010–2020 годы лица,
совершившие преступления террористического характера

В информационной среде развернулось весьма активное противоборство между государственными органами и запрещенными группировками. Данные группировки, как правило, под псевдонимами пропагандируют запрещенные идеологии в сети Интернет[1]. Государственные регуляторы, оказывая им противодействие, блокируют сайты и страницы в социальных сетях с подозрительным и опасным контентом экстремистского характера, вычисляют местонахождение распространителей информации террористической направленности.

[1] Харисова З. И. Международно-правовые основы информационной безопасности в целях устойчивого развития // Правовое обеспечение развития социального государства в свете целей устойчивого развития : сборник материалов Международной научно-практической конференции (Уфа, 12–13 ноября 2018 г.). В 2-х ч. : ч. 2. – Уфа : РИЦ БашГУ, 2018. – С. 103–106.

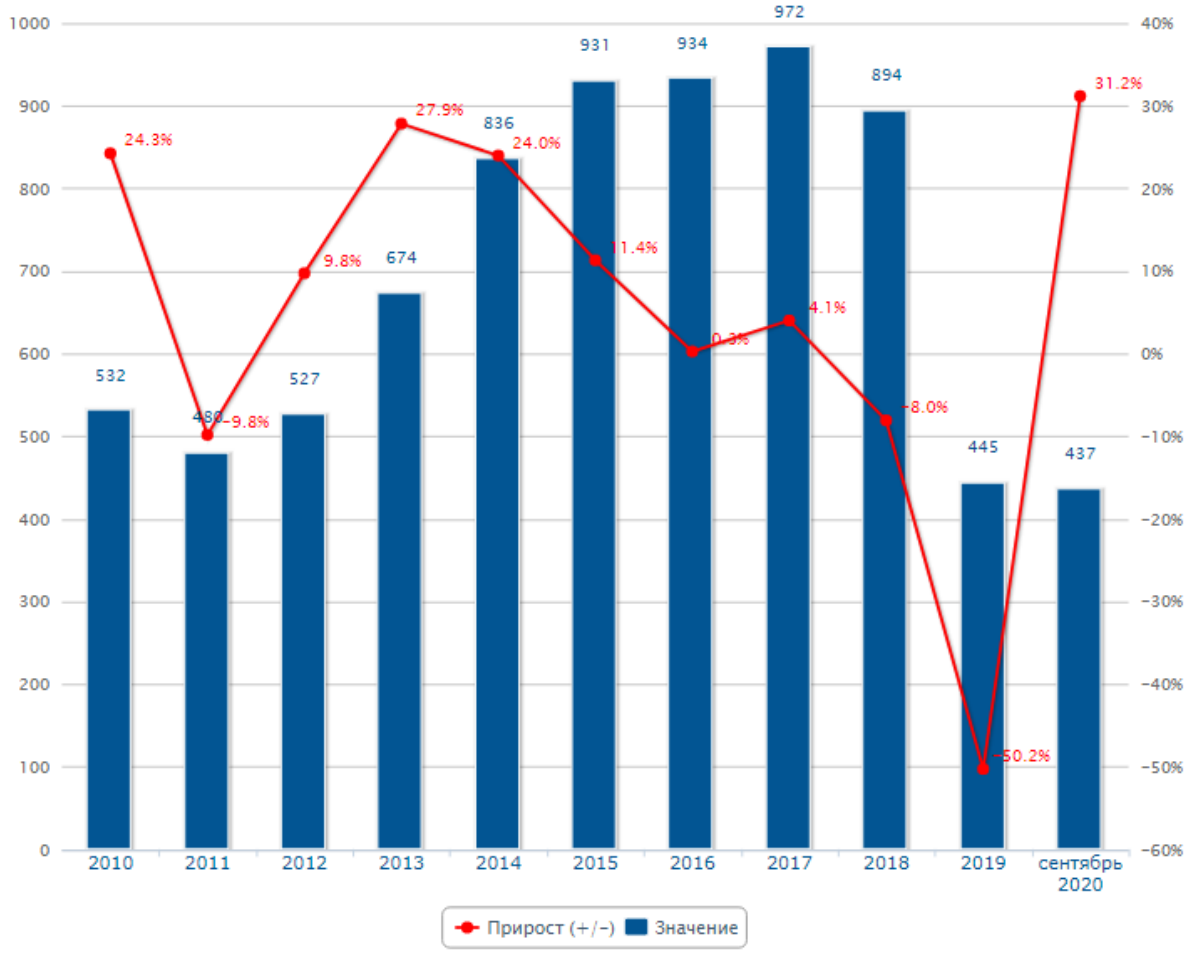

Рис. 5. Зарегистрированные за 2010–2020 годы лица,
совершившие преступления экстремистского характера

Но, к сожалению, информационная среда развивается настолько интенсивно, что государство не всегда успевает брать под свой контроль все сферы распространения такого рода взглядов, так как стремительно развиваются средства криптографии и маскировки значимой информации в большом потоке данных.

Также с развитием криптовалютного рынка[1] экстремистские и террористические организации могут управлять денежными средствами и целыми финансовыми потоками по защищенным каналам передачи данных, что затрудняет контроль за данными операциями со стороны государства и силовых структур.

Главенствующую роль в профилактике данных проблем занимает необходимость своевременного и эффективного развития технического

[1] Харисова З. И. Программно-аналитический комплекс «Киберпреступность» : программа для ЭВМ; правообладатель ФГКОУ ВО Уфимский ЮИ МВД России. 2020660996; заявл. 23 сентября 2020 г.; опубл. 30 сентября 2020 г.

обеспечения безопасности информационных сетей, находящихся в руках государства, в том числе силовых структур. Немаловажную роль в решении данных проблем занимает получение силовыми структурами сведений для доступа к пользовательским социальным сетям, что особенно актуально для зарубежных сетей, серверы данных которых расположены за пределами Российской Федерации.

В связи с чем предлагается использование современных методов интеллектуализации и автоматизации с целью повышения эффективности управления в ОВД.

Одной из возможных мер использования технологий искусственного интеллекта в сфере противодействия терроризму является комплексная реализация интеллектуальной системы мониторинга интернет-трафика, состоящей из подсистем регулирования государственной и региональной магистралей интернет-трафика (в том числе мобильного), телефонии и телевидения.

При условии своевременной актуализации ключевых слов, используемых кибертеррористами, а также проведения тщательных разведывательных мероприятий на уровне силовых структур, возможно построение модели, аналогично модели больших данных с выявлением нейронных связей между подсистемами, которые будут однозначно идентифицировать абонентов сетей в рамках обнаружения противоправных деяний с графическим отображением карты взаимодействий абонентов.

Предлагаемая система позволит оперативно реагировать на аномальную деятельность в пределах локальных сетей пользователей, а также в сетевых процессах, кроме того, позволит автоматизировать часть рутинной деятельности администраторов безопасности информационно-телекоммуникационных сетей.

Одной из основных целей экстремизма и терроризма является создание атмосферы общественной напряженности и страха посредством воздействия на общество. Посредством глобальной сети и социальных сетей экстремистские и террористические организации осуществляют вербовку новых членов, жертвой чего главным образом становится молодежь. Так, информационный аспект терроризма и экстремизма играет существенную роль. Агрессия, культ насилия, которые публикуются в глобальной сети и в социальных сетях, негативно влияют на общество и в первую очередь на молодое поколение с неустоявшимися жизненными ориентирами.

По этой причине важное значение имеет профилактическое воздействие глобальной сети и социальных сетей в снижении уровня напряженности, агрессии, социальной тревожности и страха, в воспитании молодежи и общества в духе мира и конструктивного взаимодействия, обозначения истинного предназначения религиозных течений.

С учетом обозначенного можно сделать вывод, что одним из главных направлений в условиях столь масштабной активизации международных

террористических организаций является установление сотрудничества и формирование единого нормативно-правового пространства в сфере противодействия информационному терроризму. Также можно отметить, что Российская Федерация первой в мире ратифицировала все 13 универсальных антитеррористических конвенций организации объединенных наций (ООН).

Использование информационно-телекоммуникационных технологий в террористических целях, а также для деструктивного воздействия на критическую информационную инфраструктуру государства, для распространения идеологии терроризма является одной из основных угроз в области международной информационной безопасности.

Выработка единого подхода к прекращению функционирования ресурсов террористического характера в глобальной сети Интернет, поиск и отслеживание содержимого сайтов террористической направленности, использование программного обеспечения мониторинга информационных систем и баз данных[1], своевременное проведение криминалистических экспертиз электронной техники, принятие необходимых мер законодательного и иного характера, гарантирующих доступ законным образом на территорию государств-участников к информационно-коммуникационной инфраструктуре, в отношении которой ведутся следственные действия по подозрению в террористической деятельности или деятельности, способствующей проведению террористических актов – являются основными мерами противодействия государств использованию информационного пространства в террористических целях.

При этом основными направлениями государственной политики Российской Федерации по формированию механизма противоборства информационному терроризму является организация обмена информацией о наилучших практиках в области противодействия информационному терроризму, в том числе использование систем на основе искусственного интеллекта, а также установление сотрудничества с государствами-членами Организации Договора о коллективной безопасности, государствами и Шанхайской организации сотрудничества (ШОС), государствами – участниками Содружества Независимых Государств (СНГ), группой 5 стран БРИКС (Бразилия, Россия, Индия, Китай, Южно-Африканская Республика), что будет способствовать предупреждению, выявлению, пресечению, раскрытию и расследованию актов деструктивного воздействия на элементы национальной критической информационной инфраструктуры, минимизации последствий реализации таких актов, а также противодействию

[1] Харисова З. И. Программно-аналитический комплекс «Киберпреступность» : программа для ЭВМ; правообладатель ФГКОУ ВО Уфимский ЮИ МВД России. 2020660996; заявл. 23 сентября 2020 г.; опубл. 30 сентября 2020 г.

использования глобальной сети Интернет в целях распространения идеологии терроризма.

С целью снижения затрат по ликвидации последствий от преступлений в области информационной безопасности важно заблаговременно исключать потенциально возможные угрозы[1], принимать меры по прогнозированию угроз, проводить своевременные мониторинг и анализ технологий передачи и обработки данных на предмет уязвимостей.

В заключение необходимо отметить, что развитие информационных технологий открывает целый спектр возможностей внедрения различных комплексов аппаратных программ для успешной реализации государственной политики в сфере внутренних дел, улучшения и координации взаимодействия между структурными подразделениями МВД России, а так же для быстрого и точного расследования преступлений как в информационной среде, так и общей направленности.

[1] Антонов В. В., Куликов Г. Г., Харисова З. И. Теоретико-множественный подход к построению дуальной системной модели ПАК для исследуемой области деятельности со смешанными реальными и виртуальными объектами // Вестник Южно-Уральского государственного университета. – 2019. – № 1. – С. 5–15.

ЗАКЛЮЧЕНИЕ

Современный динамичный мир требует своевременной реакции всех социальных систем, в первую очередь социальных систем, от которых зависит жизнеспособность общества и государства. Наука управления призвана выявлять направления развития, оптимизации, повышения эффективности управляемых систем. Более того, отдельные направления науки выработали эффективную методологию, позволяющую качественно повысить все этапы управления, начиная от прогнозирования, заканчивая контролем исполнения управленческих решений и реализации всего цикла управления. Современные технологии также вносят существенный вклад в управленческую деятельность: системы поддержки принятия решений, основанные на методах искусственного интеллекта, прогноз на основе нейронных сетей и других методах машинного обучения и т. д.

Информационные технологии – это совокупность методов и средств целенаправленного изменения каких-либо свойств информации. Информационная технология сферы управления предъявляет самые высокие требования к «человеческому фактору», оказывая принципиальное влияние на квалификацию работника. Информационная технология является важной составляющей процесса использования информационных ресурсов.

Автоматизированная информационная технология управления – система методов и способов сбора, накопления, хранения, поиска, обработки и защиты управленческой информации на основе применения развитого программного обеспечения, средств вычислительной техники и связи, а также способов, с помощью которых эта информация предоставляется пользователям. Новые информационные технологии связаны с информационным обеспечением процесса управления в режиме реального времени. Новая информационная технология – это технология, которая основывается на применении компьютеров, активном участии пользователей в информационном процессе, высоком уровне дружественного пользовательского интерфейса, широком применении пакетов прикладных программ общего и проблемного направления, использовании режима реального времени и доступа пользователя к удаленным базам данных и программам благодаря компьютерным сетям.

Исходя из вышесказанного можно сделать вывод, что управление предполагает реализацию ряда функций, под которыми понимаются определенные направления деятельности по выполнению задач управления ОВД посредством информационно-телекоммуникационных технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

I. Официальные документы и нормативно-правовые акты

1. **Российская Федерация. Законы.** О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации : Федеральный закон от 30 ноября 2011 г. № 342-ФЗ : текст с изменениями и дополнениями на 8 декабря 2020 г. // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 20.01.2022). Текст : электронный.

2. **Российская Федерация. Законы.** О содержании под стражей подозреваемых и обвиняемых в совершении преступлений : Федеральный закон от 15 июля 1995 № 103-ФЗ : текст с изменениями и дополнениями на 27 января 2020 г. // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 19.01.2022). Текст : электронный.

3. **Российская Федерация. Законы.** О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера : Федеральный закон от 21 декабря 1994 г. № 68-ФЗ : текст с изменениями и дополнениями на 27 января 2020 г. // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 20.01.2022). Текст : электронный.

4. **Российская Федерация. Законы**. О полиции : Федеральный закон от 7 февраля 2011 г. № 3-ФЗ : текст с изменениями и дополнениями на 6 февраля 2020 г. // Информационно-правовой портал «Гарант.ру». URL: https://base.garant.ru/ (дата обращения: 21.01.2022). Текст : электронный.

II. Статьи из газет, журналов

1. **Безруков, А. В.** Взаимодействие органов внутренних дел с другими органами публичной власти в сфере обеспечения правопорядка // Проблемы правоохранительной деятельности. 2016. № 4. С. 117–122. Текст : непосредственный.

2. **Жерновой, М. В.** Совершенствование взаимодействия органов государственной власти субъектов РФ и местного самоуправления с территориальными подразделениями полиции // Муниципальная служба : правовые вопросы. 2011. № 3. С. 23−26. Текст : непосредственный.

3. **Харисова, З. И., Сайнеев, В. Е.** Отдельные аспекты противодействия экстремизму и терроризму в сети Интернет // Идеалы и ценности ислама в образовательном пространстве XXI века : материалы Международной научно-практической конференции, приуроченной к 30-летию открытия первого в постсоветском пространстве мусульманского медресе при

ЦДУМ России имени Ризаэтдина бинэ Фахретдина (Уфа, 23 октября 2019 г.). Уфа : Печать, 2019. С. 367–370. Текст : непосредственный.

4. Сборник о состоянии преступности в России (2010–2020 гг.) Информационно-аналитический портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/analytics (дата обращения: 18.01.2022). Текст : электронный

5. **Харисова, З. И.** Актуальные проблемы деятельности правоохранительных органов по противодействию преступности в глобальной сети Интернет // Вестник Уфимского юридического института МВД России. 2019. № 3. С. 92–97. Текст : непосредственный.

6. **Харисова, З. И.** Международно-правовые основы информационной безопасности в целях устойчивого развития // Правовое обеспечение развития социального государства в свете целей устойчивого развития : сборник материалов Международной научно-практической конференции (Уфа, 12–13 ноября 2018 г.). В 2 ч. : ч. 2. Уфа : РИЦ БашГУ, 2018. С. 103 – 106. Текст : непосредственный.

7. **Харисова, З. И., Филиппов, О. А.** Международное сотрудничество в области противодействия экономическим преступлениям с использованием криптовалют // Организация Объединенных Наций и глобальные проблемы человечества в XXI веке : материалы Международной научно-практической конференции 15 ноября 2019 г. Уфа : РИЦ БашГУ, 2019. С. 256–263. Текст : непосредственный.

8. **Харисова, З. И.** Программно-аналитический комплекс «Киберпреступность» : программа для ЭВМ; правообладатель ФГКОУ ВО Уфимский ЮИ МВД России. 2020660996; заявл. 23 сентября 2020 г.; опубл. 30 сентября 2020 г.

9. **Харисова, З. И.** «БАЗИС – Базовый анализ защищенности информационных систем» : программа для ЭВМ; правообладатель ФГКОУ ВО Уфимский ЮИ МВД России. 2020666679; заявл. 17 декабря 2019 г.; опубл. 15 января 2020 г.

10. **Fetisov V, Kharisova Z, Dmitriyev O and Melnichuk O.** Rapid particle size analysis of suspensions based on video technology and artificial neural network with additional training during operation // International Journal of Applied Engineering Research. Vol 12 (7). P. 1271. Текст : непосредственный.

11. **Антонов, В. В., Куликов, Г. Г., Харисова, З. И.** Теоретико-множественный подход к построению дуальной системной модели ПАК для исследуемой области деятельности со смешанными реальными и виртуальными объектами // Вестник Южно-Уральского государственного университета. 2019. № 1. С. 5–15. Текст : непосредственный.

III. Учебники, учебные пособия, словари

1. **Аврутин, Ю. Е.** Основы управления в органах внутренних дел : учебник для вузов / Ю. Е. Аврутин [и др.]; под общей редакцией Ю. Е. Аврутина. 2-е изд., перераб. и доп. Москва : Юрайт, 2019. 249 с. (Специалист). ISBN 978-5-534-06242-7 // ЭБС Юрайт. URL: https://biblio-online.ru/bcode/437996 (дата обращения: 20.01.2022). Текст : электронный.

2. **Анисимов, В. Л.** Участие органов внутренних дел в чрезвычайных ситуациях и обстоятельствах : теоретический и правовой аспекты : монография / В. Л. Анисимов. – Москва : Всерос. науч.-исслед. ин-т МВД России, 2001. 93 с. Текст : непосредственный.

3. **Анташов, В. А.** Основы предпринимательского дела : Благород. бизнес : учебник для вузов по направлениям «Экономика» и «Менеджмент» // В. А Анташов, В. Г. Варшамова, Е. С. Зотова [и др.]; под рук. и ред. Ю. М. Осипова, Е. Е. Смирновой. 2-е изд., перераб. и доп. Москва : Бек, 1996. 459 с. (В пер.). ISBN 5-85639-143-8 // ЭБС Юрайт. URL : https://search.rsl.ru/ru/record/01001748235. Текст : электронный.

4. **Афанасьев, В. Г.** Общество : системность, познание и управление : (системность и гносеология, системность и управление) / В. Г. Афанасьев. Москва : URSS, cop. 2019. 431 с. ISBN 978-5-9710-6576-0. Текст : непосредственный.

5. **Бавсун, И. Г.** Основы управления в органах внутренних дел : учебное пособие / И. Г. Бавсун. Омск : ОмА МВД России, 2017. 150 с. ISBN 978-5-88651-647-0 // ЭБС Юрайт. URL: https: be5.biz/pravo/a016/index.html. Текст : электронный.

6. **Бахрах, Д. Н.** Административное право : учебник для вузов / Д. Н. Бахрах. Москва : Бек, 1996. 355 с. ISBN 5-85639-135-7 // ЭБС Юрайт. URL: https://search.rsl.ru/ru/record/01004965453. Текст : электронный.

Учебное издание

Антонов Вячеслав Викторович
(доцент, доктор технических наук)
Харисова Зарина Ирековна
(кандидат технических наук)
Калимуллин Наиль Расфарович
(б/с, б/з)
и др.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Редактор Р. Р. Гафарова

Подписано в печать 15.03.2022	Выход в свет 28.03.2022
Гарнитура Times	Формат 60x84 1/16
Уч.-изд. 2,8 л.	Усл. печ. 3 л.
Тираж 70 экз.	Заказ № 3

Редакционно-издательский отдел
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2

Отпечатано в группе полиграфической и оперативной печати
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2