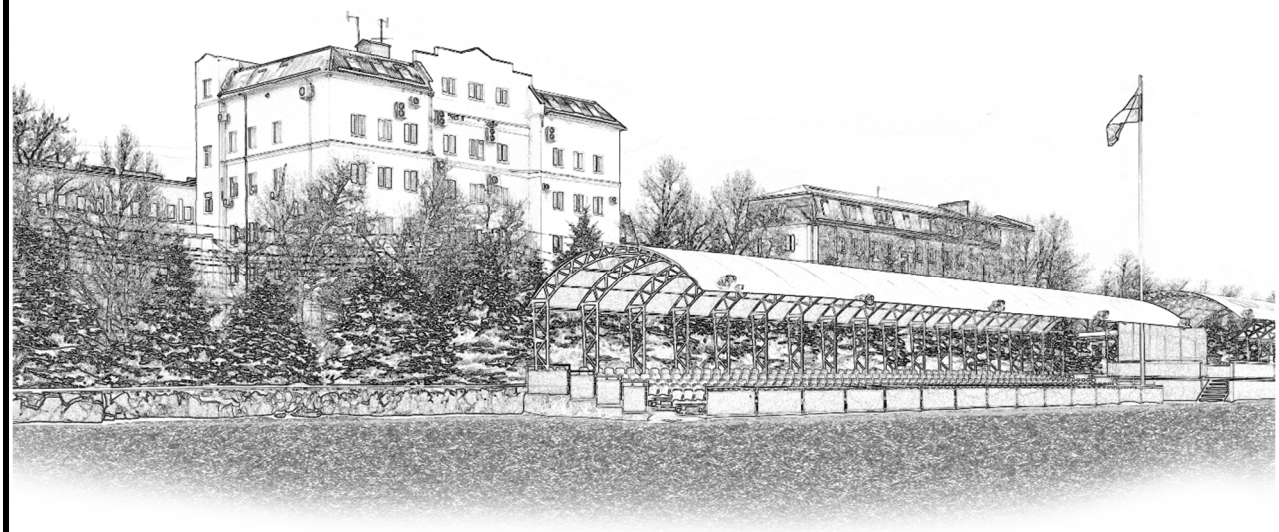
Краснодарский университет МВД России

Д. С. Богданов
А. В. Еськов

Использование органами внутренних дел специализированного российского программного обеспечения для поиска сведений о физических и юридических лицах в открытых источниках сети Интернет



Краснодар
2023

Краснодарский университет МВД России

Д. С. Богданов
А. В. Еськов

Использование органами внутренних дел специализированного российского программного обеспечения для поиска сведений о физических и юридических лицах в открытых источниках сети Интернет

Учебное пособие

Краснодар
2023

УДК 303.645.063
ББК 16.23
Б734

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:
Т. В. Мещерякова, доктор технических наук, доцент (Воронежский институт МВД России);
Н. А. Капусткин (Московский университет МВД России имени В. Я. Кикотя).

Богданов Д. С.
Б734 Использование органами внутренних дел специализированного российского программного обеспечения для поиска сведений о физических и юридических лицах в открытых источниках сети Интернет : учебное пособие / Д. С. Богданов, А. В. Еськов. – Краснодар : Краснодарский университет МВД России, 2023. – 76 с.

ISBN 978-5-9266-1921-5

Содержится описание специализированного программного обеспечения, используемого для поиска сведений о физических и юридических лицах в открытых источниках сети Интернет.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 303.645.063
ББК 16.23

ISBN 978-5-9266-1921-5

Введение

С появлением новых информационных технологий, основанных на широком внедрении средств компьютерной техники и систем телекоммуникации, информация становится постоянным и необходимым атрибутом обеспечения деятельности государств, общественных объединений, юридических лиц и простых граждан. Местом создания, обработки, хранения и распространения различного рода информации стали стремительно растущие компьютерные сети, в числе которых сеть Интернет. Сегодня интернет-ресурсы занимают лидирующее положение среди всех остальных традиционных средств массовой информации. В ряде случаев Интернет становится основным, а порой и единственным, источником информации. Благодаря Интернету большое количество людей имеют реальную возможность приобщиться к огромному массиву накопленной информации и достаточно часто пользуются этим благом (помещают в сеть и хранят в ней фото-, видео- и аудиоматериалы, осуществляют интернет-покупки с использованием бесконтактных банковских платежных систем, обмениваются информацией посредством электронной почты и многое другое).

Повышенный интерес к Интернету стали проявлять не только законопослушные граждане, но и преступные элементы, которые для достижения, прежде всего, корыстных целей начали

активно использовать компьютерную технику, современные информационные технологии и компьютерные сети. Одновременно наблюдается резкое нарастание криминального профессионализма во время исполнения преступлений, появились новые их виды, постоянно обновляются способы совершения преступлений, увеличивается их количество и тяжесть последствий.

По данным отчета МВД России о состоянии преступности в Российской Федерации за январь – декабрь 2022 г., зарегистрировано 522,1 тыс. преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. В общем числе зарегистрированных преступлений их удельный вес увеличился с 25,8% в январе – декабре 2021 г. до 26,5%. Практически все такие преступления (98,7%) выявляются органами внутренних дел. Больше половины таких преступлений (52,1%) относятся к категориям тяжких и особо тяжких (272,2 тыс.; -5,6%), почти три четверти (73,0%) совершается с использованием сети Интернет (381,1 тыс.; +8,4%), более трети (40,8%) – средств мобильной связи (213,0 тыс.; -2,1%) [1]. Такие статистические данные говорят о том, что практически каждое четвертое преступление совершается с использованием информационно-телекоммуникационных технологий, и их удельный вес продолжает ежегодно расти.

В связи с большим количеством компьютерных атак, дистанционным хищением денежных средств и активным развитием противоправной цифровой индустрии, а также во исполнение Указа Президента РФ от 30.09.2022 № 688 «О внесении изменений в некоторые акты Президента Российской Федерации» в структуре МВД России создано Управление по организации борьбы с противоправным использованием информационно-коммуникационных технологий (УБК МВД России), в ГУ МВД и УМВД по субъектам Российской Федерации созданы отделы по расследованию преступлений в сфере информационных технологий. Одной из основных задач Управления [2] является анализ данных, содержащихся в информационно-телекоммуникационных сетях, в целях выявления запрещенного контента и противодействия IT-преступности.

Необходимым условием успешной работы по выявлению, пресечению, раскрытию и расследованию преступлений, совер-

шаемых с использованием информационных технологий, и поиску сведений о физических и юридических лицах – участниках преступления является понимание сотрудниками органов внутренних дел специфики функционирования киберсреды, ее трансграничного характера, умение работать в сфере высоких информационных технологий, взаимодействовать с представителями IT-компаний и другими специалистами, знание, как и где искать доказательства, как их правильно фиксировать, особенно, если речь идет о цифровых следах преступлений.

В данном учебном пособии приведены наиболее популярные ресурсы и сервисы, предназначенные для сбора информации о физических и юридических лицах в открытых источниках сети Интернет, описаны их функциональные возможности, даны методические рекомендации по выбору специализированного поискового программного обеспечения, наиболее подходящие для решения задач, стоящих перед органами внутренних дел по поиску вышеуказанных сведений.

Использование подобного рода поискового программного обеспечения позволит многократно упростить и ускорить работу по сбору сведений о физических и юридических лицах, что, в свою очередь, может повысить эффективность работы сотрудников органов внутренних дел, специализирующихся на выявлении, пресечении, раскрытии и расследовании преступлений.

Глава 1. Развитие направления использования специализированного программного обеспечения в деятельности органов внутренних дел

1.1. Актуальность использования специализированного программного обеспечения в интересах органов внутренних дел

Как показывает практика противодействия киберпреступности, при осуществлении отдельных оперативно-розыскных мероприятий, проведении доследственной проверки или следственных действий по IT-преступлениям предполагается поиск информации о физических и юридических лицах, представленной в текстовом, графическом, видео- или аудиоформате. Для каждого из этих типов данных существуют особенности их обнаружения и исследования.

Выделяются несколько направлений получения информации из киберпространства [3].

1. Получение информации по запросу к соответствующим организациям. Наведение справок является одним из наиболее часто проводимых оперативно-розыскных мероприятий, позволяющим получить достоверную информацию о физическом или юридическом лице из официальных источников. К таким источникам относятся, например, провайдеры сотовой связи или Интернета, налоговые и финансовые учреждения, учреждения труда и здравоохранения и множество других, располагающих различными сведениями, в том числе составляющими различные виды тайн, о лицах, интересующих правоохранительные органы. Подобное получение информации предполагает санкционирование нарушения прав физических или юридических лиц на сохранение в тайне информации, распространение которой ограничено на основании федеральных законов, и осуществимо в рамках официальных запросов правоохранительных органов в соответствующие государственные и негосударственные органы или учреждения.

2. Получение информации с помощью технических средств. При расследовании преступлений средней тяжести, тяжких или особо тяжких, в случаях необходимости нарушения конституци-

онных прав человека и гражданина, на основании ст. 8 Федерального закона 12.08.1995 № 144-ФЗ (в редакции от 28.12.2022) «Об оперативно-розыскной деятельности» допускается использование технических средств негласного получения и информации в рамках следующих оперативно-розыскных мероприятий: прослушивание телефонных переговоров, снятие информации с технических каналов связи, получение компьютерной информации; а также при проведении оперативно-технических мероприятий: негласная аудиозапись, негласное видеонаблюдение, негласное видеодокументирование [3]. Проведение таких мероприятий требует обязательного судебного санкционирования, наличия специальных технических средств и дополнительного времени на расшифровку и фиксацию получаемых сведений, что существенно увеличивает срок проведения оперативно-розыскных мероприятий. Оперативным подразделениям также необходимо проводить дополнительные процессуальные действия по приведению результатов оперативно-розыскных мероприятий в доступный вид для ознакомления органом дознания, следствия или суда, увеличивая срок предварительного расследования.

3. Получение информации из общедоступных источников. Сведения, оставляемые пользователем в сети Интернет в процессе получения доступа к определенным ресурсам, общения, взаимодействия с другими пользователями, демонстрации созданного контента и в других целях, называются цифровым следом. С увеличением числа пользователей интернет-ресурсами и их активности при работе в различных приложениях растет и объем сведений, связанных с тем или иным лицом.

OSINT (Open source intelligence) – поиск, выбор и сбор информации по общедоступным источникам, т. е. проведение разведки с использованием находящейся в открытом доступе информации, которая собирается с целью последующего анализа [4–7, 12, 26]. Источниками информации в этом случае могут являться:

− средства массовой информации (газеты, журналы, радио, телевидение);

− интернет-ресурсы: социальные сети, блоги, форумы, чаты, каналы мессенджеров – весь размещенный контент (текст, фото-, аудио- и видеоматериалы);

− публичные отчеты различных организаций, правительства, официальные данные о бюджете, демографии; пресс-конференции, брифинги, публичные заявления;

− наблюдения – радиомониторинг, данные карт, аэрофотосъемок, дистанционного зондирования земли;

− научные и профессиональные отчеты различных организаций, доклады, конференции, статьи.

С технической точки зрения преимущество расследования с помощью открытых источников заключается в отсутствии необходимости располагать специальными знаниями в сфере информационных технологий, дорогостоящими техническими и программными средствами для получения необходимого результата. Современные ресурсы позволяют получить достаточный объем сведений без дополнительных вложений и навыков.

Существует два основных метода поиска и сбора информации, выбор которого зависит от исходных данных и условий и необходимого результата проводимого исследования.

1. Пассивный – наиболее распространенный метод, который ограничивается анализом доступной информации, архивной или сохраненной на интернет-ресурсе. Пассивный метод поиска информации также характеризуется большим объемом получаемой информации, которая нуждается в проверке на актуальность и достоверность ввиду избыточности. Лицо, осуществляющее поиск подобной информации, оставляет проводимую разведку в тайне и не позволяет себя обнаружить.

2. Активный метод предполагает применение специальной техники и программного обеспечения, взаимодействие происходит непосредственно с системой, в которой находится значимая информация. Зачастую активный метод разведки предполагает внедрение в информационную систему с помощью отдельных или уже существующих учетных записей, действия которых документируются в системных журналах, в результате чего разведывательная деятельность может быть обнаружена и предупреждена. Применение социальной инженерии также расценивается как активный сбор информации, поскольку предполагает непосредственный контакт с лицом, располагающим необходимыми сведениями.

Осуществление поиска информации в открытых источниках сети Интернет характеризуется значительной вариативностью и наличием специфических особенностей. А методы его производства существенно различаются как по типу извлекаемой информации, так и по эффективности, качеству и результативности.

Отдельным и основным преимуществом осуществления поиска информации по открытым источникам является отсутствие необходимости оперативным подразделениям санкционировать действия по поиску необходимой информации, т. е. осуществлять разведывательную деятельность самостоятельно. При осуществлении сбора информации из открытых источников отсутствует необходимость получения разрешения на копирование, распространение и передачу информации, поскольку ее размещение в открытых источниках предполагает согласие обладателя информации на свободное распространение публикуемых сведений вне зависимости от целей. Таким образом, значительно снижается нагрузка, связанная с необходимостью санкционирования деятельности оперативных и следственных подразделений и оформления процессуальных документов, связанных с передачей материалов дела органам дознания, следствия и в суд.

В общем случае OSINT – это один из многих видов сбора данных из открытых источников, который дополняется следующим.

1. Человеческий интеллект (HUMINT) – получение информации от человека в указанном месте. Примеры источников информации – это персонал организации, интересующей сотрудника ОВД, опрос граждан патрулирующими сотрудниками.

2. GEOINT – сбор информации с помощью спутниковой и аэрофотосъемки или карт местности; IMINT – получение интеллектуальных изображений.

4. Информация в виде интеллектуальных измерений и сигнатур, собираемых из массива сигнатур (отличительных характеристик) фиксированных или динамических целевых источников – MASINT, разделена на шесть основных дисциплин: электрооптические, ядерные, радарные, геофизические, материалы и радиочастотные.

5. Информация, выделяемая из интеллектуальных сигналов (SIGINT), собирается в результате перехвата сигналов: коммуникационная разведка (COMINT); электронная разведка (ELINT) –

собирается из электронных сигналов, не содержащих речи или текста; радиотехническая разведка FISINT – влечет за собой сбор и анализ телеметрических данных внешней аппаратурой (ранее известная как телеметрическая разведка TELINT).

6. Информация, собираемая на основе анализа оружия и оборудования, используемого вооруженными силами иностранных государств, или условий окружающей среды – TECHNINT.

7. Медицинские данные (MEDINT) – данные, собранные на основе анализа медицинских карт.

8. Информация, получаемая с использованием цифрового сетевого интеллекта (CYBINT или DNINT) собирается из киберпространства.

9. Информация, собираемая из анализа денежных транзакций, – FININT.

Указанные виды проведения сбора информации дополняют возможности получения информации методами OSINT.

1.2. Направления использования специализированного программного обеспечения для поиска информации в сети Интернет

При осуществлении расследования административных и уголовных дел сотрудникам необходимо собирать, обобщать, фиксировать и анализировать значительный объем информации, связанный с совершенным правонарушением. Так, в рамках административного или уголовного правонарушения необходимо обладать актуальными и достоверными данными по основным элементам состава правонарушения или преступления, а именно его объективными и субъективными признаками. Данная информация может содержать следующие сведения:

– персональные данные подозреваемого, потерпевшего или свидетелей;

– сведения о предмете или орудии совершения преступления;

– сведения о размере причиненного ущерба;

– внешнее описание подозреваемого, потерпевшего или свидетелей;

– фиксированный факт совершения преступления или правонарушения;

– дату, время, место, способ и другие сведения, составляющие объективную сторону совершенного преступления или правонарушения в целом.

В современных тенденциях индустриального общества информационные технологии так или иначе встречаются в каждом элементе состава преступления, что обусловливает острую необходимость овладения и применения сотрудниками специальных знаний в данной сфере.

В органах внутренних дел отмечается значительный недостаток кадров, обладающих знаниями в сфере применения информационных технологий, а также специальных технических средств для осуществления различных мероприятий по получению значимой для расследования информации. В связи с данными факторами все чаще самими сотрудниками принимаются меры по минимизации использования специализированных средств, а также обращений к компетентным специалистам в данной сфере, а именно – самостоятельный поиск необходимых сведений на просторах сети Интернет.

Упрощение поиска информации о событиях или участниках совершенного правонарушения или преступления обусловлено повсеместной популяризацией социальных сетей, а также иных информационных технологий, используемых людьми ежедневно. К таким технологиям, помимо социальных сетей, можно отнести различные мессенджеры, навигаторы, файлообменные серверы, сервисы электронной почты, логистические сервисы и др. Подобные сервисы располагают значительным объемом информации о пользователе, позволяя по некоторым косвенным признакам идентифицировать его с наибольшей вероятностью совпадения.

Разведка на основании открытых источников является достаточно молодой отраслью системного анализа и обобщения информации, однако сопоставление известных данных и получение определенных выводов так или иначе является базовым свойством человеческого разума. OSINT представляет собой совокупность методов, предназначенных для целевого поиска, обобщения

и всестороннего анализа всех открытых данных об интересующем объекте.

Активное пользование социальными сетями обусловливает обилие информации, размещаемое самими владельцами в сети Интернет. Так, обладая знаниями о том, как человек выглядит, или его имени и фамилии, можно узнать его дату рождения, город проживания, место получения образования, а также легко установить круг его близких друзей и знакомых.

Зачастую поиск подобной информации не представляется трудной задачей не только для сотрудников органов внутренних дел, но и для обычных пользователей сети Интернет. В рамках деятельности правоохранительных органов существует проблема приобщения информации, получаемой в открытых источниках, к уголовному или административному делу, по которому непосредственно ведется производство и в рамках которого осуществлен поиск данных.

Проблема придания юридической и правовой силы материалам, размещенным в сети Интернет, является ключевой при использовании информационных технологий в процессе осуществления сбора информации по административным или уголовным делам [8]. Так, в случае проведения предварительного расследования с использованием OSINT по открытым источникам говорят о следующих оперативно-розыскных мероприятиях.

1. Сбор образцов для сравнительного исследования. В рамках проведения данного оперативно-розыскного мероприятия в открытых источниках можно получить сведения об интересующем предмете исследования, в особенности при решении задачи установления принадлежности предмета или орудия преступления конкретному лицу.

2. Наблюдение. Наблюдение по активности в сети Интернет является достаточно новой отраслью ведения разведывательной деятельности, однако в современных реалиях обладает достаточной достоверностью в сочетании с простотой осуществления: многие пользователи сети Интернет склонны часто публиковать контент о собственном времяпрепровождении в режиме онлайн, а также с помощью социальных сетей можно наблюдать некоторые события, произошедшие с пользователем ранее.

3. Отождествление личности. Проведение отождествления личности посредством социальных сетей и интернет-ресурсов в целом является простым и быстрым методом идентификации интересующего правоохранительные органы лица. С помощью таких средств, как сервисы поиска по фото, можно сопоставить имеющееся изображение человека с его персональными данными, например фамилией, именем, отчеством, датой рождения и др., и наоборот.

4. Получение компьютерной информации. Данное оперативно-разыскное мероприятие представляет собой совокупность действий, направленных на получение каких-либо цифровых данных, относимых к расследуемому уголовному делу. Компьютерная информация представляет собой любые данные, обрабатываемые электронно-вычислительной машиной, данное мероприятие напрямую связано с осуществлением поиска информации в открытых источниках сети Интернет, поскольку методы такой разведки используют специальные программные средства.

Стоит отметить, что наведение справок, несмотря на кажущееся сходство с разведкой по открытым источникам, имеет принципиальное отличие от данного метода получения информации. В первую очередь, наведение справок – установленное федеральным законом оперативно-розыскное мероприятие, проводимое на основании соответствующих процессуальных решений и соответствующих им процессуальных документов. Проведение разведки в открытых источниках подразумевает отсутствие необходимости санкционирования деятельности по поиску необходимой информации с руководителем подразделения или сотрудником органа следствия или дознания. Данный факт также означает, что результаты проведенной разведки по открытым источникам не нуждаются в рассекречивании как результаты оперативно-розыскной деятельности для передачи органу дознания, следствия или в суд.

Использование проведения исследования информации в открытых источниках также может использоваться в качестве подтверждения или опровержения информации, полученной от агентурного аппарата или в результате такого следственного действия, как допрос, или оперативно-розыскного опроса. Используемые в ходе данного мероприятия сведения могут иметь

всесторонний характер, а значит данный метод получения информации является универсальным.

Открытые источники информации также представляют собой обширное поле исследования для аналитической деятельности органов внутренних дел. Поскольку под открытыми источниками также понимаются опубликованные в сети Интернет отчеты организаций, органов, учреждений, статистические данные, научные и публицистические материалы, данный массив информации может быть использован для обобщения и накопления интересующих правоохранительные органы сведений.

Контрольные вопросы

1. Какие вы знаете направления получения информации из киберпространства?
2. В чем заключается понятие термина OSINT?
3. Какие источники получения информации используются в OSINT?
4. Какие основные методы поиска и сбора информации вам известны?
5. В ходе каких оперативно-розыскных мероприятий может проводиться разведка по открытым источникам?
6. Какие ОРМ проводятся в рамках предварительного расследования с использованием OSINT?
7. Как придается юридическая и правовая сила информации, полученной из сети Интернет в процессе осуществления ее сбора по административным или уголовным делам?

Глава 2. Обзор программных средств осуществления поиска информации в открытых источниках

2.1. Обобщенные характеристики и принципы работы поискового программного обеспечения

Условиями успешной работы сотрудников ОВД по выявлению, пресечению, раскрытию и расследованию преступлений являются знание возможностей поисковых систем, принципов функционирования, специфики построения запросов и умение пользоваться специализированным программным обеспечением для поиска необходимых сведений в сети Интернет.

Поисковые системы могут быть использованы в интересах органов внутренних дел при выявлении материалов или цифровых следов, содержащих признаки преступлений, представленных в той или иной степени в Особенной части Уголовного кодекса Российской Федерации (УК РФ), в том числе совершаемых с использованием информационно-телекоммуникационных технологий, например:

– приготовление к преступлению и покушение на преступление (ст. 30 УК РФ);

– убийство (ст. 105 УК РФ);

– содействие террористической деятельности (ст. 205.1 УК РФ);

– публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ);

– массовые беспорядки (ст. 212 УК РФ);

– публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ);

– публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 280.1 УК РФ);

– публичные действия, направленные на дискредитацию использования Вооруженных сил РФ в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности или исполнения государственными

органами Российской Федерации своих полномочий в указанных целях (ст. 280.3 УК РФ);

– возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 282 УК РФ);

– организация экстремистского сообщества (ст. 282.1 УК РФ);

– организация деятельности экстремистской организации (ст. 282.2 УК РФ);

– финансирование экстремистской деятельности (ст. 282.3 УК РФ);

– призывы к введению мер ограничительного характера в отношении Российской Федерации, граждан Российской Федерации или российских юридических лиц (ст. 284.2 УК РФ);

– реабилитация нацизма (ст. 354.1 УК РФ);

В свою очередь, в Кодексе Российской Федерации об административных правонарушениях (КоАП РФ) закреплены следующие преступления:

– возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (ст. 20.3.1 КоАП РФ);

– злоупотребление свободой массовой информации (ст. 13.15 КоАП РФ);

– иные преступления или правонарушения.

Ниже представлены принципы работы и обобщенные характеристики поискового программного обеспечения.

Поисковое программное обеспечение – программно-аппаратный комплекс, который предназначен для осуществления поиска в сети Интернет, отвечающий на запрос пользователя, задаваемый текстовой фразой, загруженным изображением или иными входными данными, основной задачей которого является выдача набора ссылок на страницы и сайты, страницы в социальных сетях или иную релевантную информацию, соответствующую запросу [9].

Выделяют следующие поисковые системы [9, 10].

1. Управляемые человеком, т. е. каталог сайтов, каждый пункт которого и общая их база данных сформированы вручную пользователем, следовательно, предоставляемые сведения будут значительно качественней, нежели результаты, сформированные автоматически. Однако обновление данных каталогов также вы-

полняется вручную, что существенно влияет на актуальность информации. Пример управляемой поисковой системы – каталог Rambler.

2. Поисковые роботы, состоят из трех частей: краулер (от англ. crawl – ползать), выполняющий перебор страниц сети Интернет и создающий список веб-страниц; индекс – большой архив копий веб-страниц и программное обеспечение, выполняющее анализ и оценку результатов поиска. Поскольку поисковый робот выполняет свою функцию постоянно и непрерывно, информация обладает достаточной актуальностью. Большинство современных поисковых систем являются системами данного типа.

3. Гибридные поисковые системы, представляющие собой комбинирование поисковых систем ручного управления и поисковых роботов, например Google. Такие поисковые системы позволяют сочетать преимущества данных поисковых систем.

4. Метасистемы, которые не составляют собственную базу данных, но обращаются за результатами к нескольким поисковым сервисам, например Vivisimo.

Ошибочно предположение о том, что поиск оптимальных результатов выполняется поисковыми системами в режиме реального времени. Выполнить анализ значительной части веб-пространства за несколько секунд невозможно, поскольку это достаточно сложный вычислительный процесс, требующий большого объема памяти и времени. Для занесения информации в поисковую базу данных необходимо проводить предварительную обработку и регулярное ранжирование.

Любое поисковое программное обеспечение уникально, большая часть применяемых методов индексирования и ранжирования документов являются коммерческой тайной, однако основные принципы работы поисковых систем сходны.

Общая схема работы характерна для большинства современных поисковых систем, вне зависимости от их назначения. В структуре поискового программного обеспечения (рис. 1) можно выделить следующие модули:

– поисковый робот (краулер);
– индексатор;
– база данных документов;

– модуль ранжирования;

– интерфейс пользователя.

Алгоритм работы поискового программного обеспечения можно интерпретировать следующими шагами.

1. Поисковый робот просматривает данные в сети Интернет с целью выявления новых документов для включения их в базу данных поисковой системы, называемую индексом. Процесс занесения информации называется индексированием. Поисковый робот использует наличие в документах гиперссылок на другие документы, что позволяет автоматически формировать очередь таких документов. Кроме того, поисковое программное обеспечение имеет механизм регистрации, что дает возможность владельцам сайтов вручную добавлять свои страницы в очередь на индексирование.

Таким образом, поисковый робот:

– исследует веб-страницы из списка, полученного при предыдущем исследовании сети;

– извлекает на страницах ссылки на другие веб-ресурсы;

– исследует страницы, добавляемые веб-мастерами вручную (регистрация в поисковике).

Рис. 1. Структура поискового программного обеспечения

2. Все найденные страницы помещаются в базу данных поискового программного обеспечения в определенном формате (индексируются) для последующей обработки и определения релевантности страниц. В процессе занесения информации в индекс составляется список слов документа, которые являются потенциальными ключевыми словами запросов пользователей. Каждое поисковое программное обеспечение имеет свои алгоритмы индексирования и форматы индексных файлов.

3. После формирования базы данных рассчитываются внутренние и внешние характеристики страниц для определения их релевантности и ранжирования в будущей выдаче поисковой системы в зависимости от типов входных данных, предоставляемых сотрудником ОВД, осуществляющим поисковый запрос. Алгоритм определения релевантности представляет собой математическую формулу с сотнями параметров, которые могут ежедневно меняться.

По запросу сотрудника ОВД поисковые системы позволяют обнаруживать различные сведения, например факты публикации материалов, распространение которых на территории Российской Федерации ограничено или запрещено, сведения о разыскиваемых или без вести пропавших лицах, факты совершения преступления или правонарушения, которые могут быть основанием для проведения оперативно-розыскных мероприятий (пп. 1–4 ч. 2 ст. 7 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»), поводом или основанием для возбуждения уголовного дела в зависимости от состава преступления (п. 3 ч. 1 и ч. 2 ст. 140 УПК РФ).

2.2. Комплексное программное обеспечение для поиска информации о физических и юридических лицах в сети Интернет

В интернет-пространстве достаточно много ресурсов для поиска информации о физических и юридических лицах как отечественного, так и иностранного происхождения. Далее рассматривается российское программное обеспечение для поиска сведений о физических и юридических лицах в открытых источниках сети Интернет,

предлагающееся разработчиками как комплексное решение (система, платформа) поиска, анализа и представления информации.

Приведенное программное обеспечение не является исчерпывающим, развитие информационных технологий и конкуренция обусловливает появление новых программных продуктов и совершенствование используемых на сегодняшний день.

Система распознавания лиц FindFace

FindFace – программное обеспечение, основанное на технологии распознавания лиц, разработчиком которого является российская организация NtechLab. Ранее данная разработка представляла собой веб-сервис, осуществляющий поиск людей по фотографии в социальной сети «ВКонтакте», однако после стремительного роста числа пользователей компания расширила спектр предоставляемых услуг и в данный момент предлагает программные решения для различных отраслей бизнеса и государственных органов, в том числе для органов внутренних дел Российской Федерации [11].

Алгоритм, заложенный в архитектуру программного обеспечения, способен распознавать неограниченное количество людей в кадре. Скорость и качество работы детектора не зависит от числа определяемых лиц. Технология способна работать в трудных условиях: при недостатке освещения, наличии визуальных искажений, изменении положения головы и перемене позы.

Алгоритм распознавания NtechLab работает следующим образом:

1) определение силуэта и лица в кадре или на изображении;
2) устранение возможных визуальных искажений;
3) извлечение характеристик лица;
4) верификация или идентификация лица.

Фотография или стоп-кадр из видеоряда (файла, содержащего видео) состоит из массива пикселей, каждый из которых имеет свой цвет – уникальный цветовой код в палитре RGB, представленный в виде числовых значений. Нейронная сеть анализирует изображение и формирует матрицу из RGB-значений пикселей, которая впоследствии будет сопоставляться в поисках совпадений с заранее подготовленными данными базы.

Существует и другой способ работы нейронной сети – это использование атрибутов, признаков лица, которые система определяет для себя. Анализ отдельно взятых признаков позволяет значительно сэкономить ресурсы и минимизировать вычислительную нагрузку, в отличии от анализа изображений.

Атрибуты представлены посредством различных опорных точек на глазах, носу, в уголках рта. Каждое лицо имеет свою уникальную совокупность векторов, построенных на этих точках. Данная совокупность формирует своеобразный биометрический шаблон, представляющий собой определенную последовательность числовых значений и использующийся для сопоставления с другими шаблонами.

Сеть способна определять частично скрытые лица, а также лица с учетом возрастных изменений, перемены прически, появления бороды, усов, очков.

Алгоритм анализирует кадр видеоряда (рис. 2), состоящего из кадров. Стоп-кадр из видеоряда, в свою очередь, состоит из массива пикселей, имеющих уникальный цветовой код. Цветовой код в палитре RGB представлен в виде трех числовых значений. Нейронная сеть получает на вход матрицу из RGB-значений пикселей.

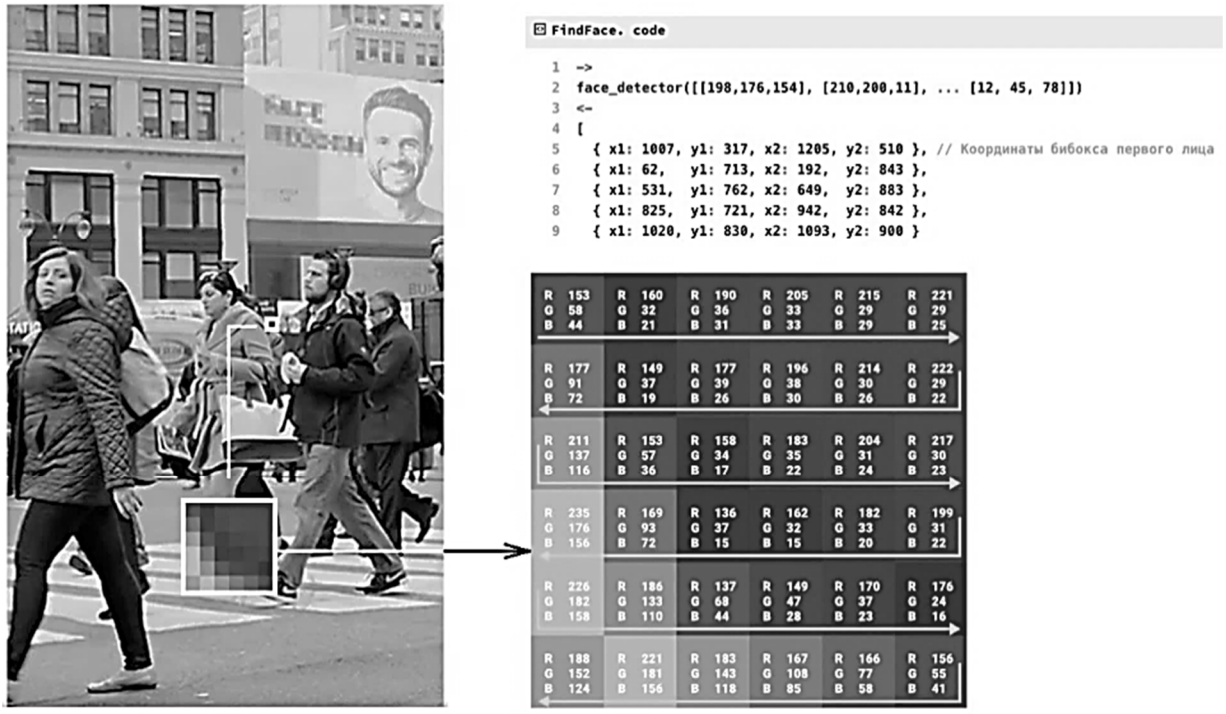


Рис. 2. Определение цветов пикселей

Алгоритм NtechLab способен определить неограниченное количество лиц в кадре, что делает его идеальным решением для обеспечения безопасности в местах массового скопления людей (рис. 3).

Рис. 3. Результат работы алгоритма обнаружения лиц

Специально созданный алгоритм способен исправить визуальные искажения: определить положение головы и, например, «развернуть» лицо в анфас (рис. 4).

Признаки лица, которые выделяет для себя система, называются атрибутами. По таким признакам можно осуществлять быстрый поиск в базах мониторинга, например найти все лица в очках. Каждый из атрибутов определяется отдельной нейронной сетью, при этом все задействованные сети работают параллельно.

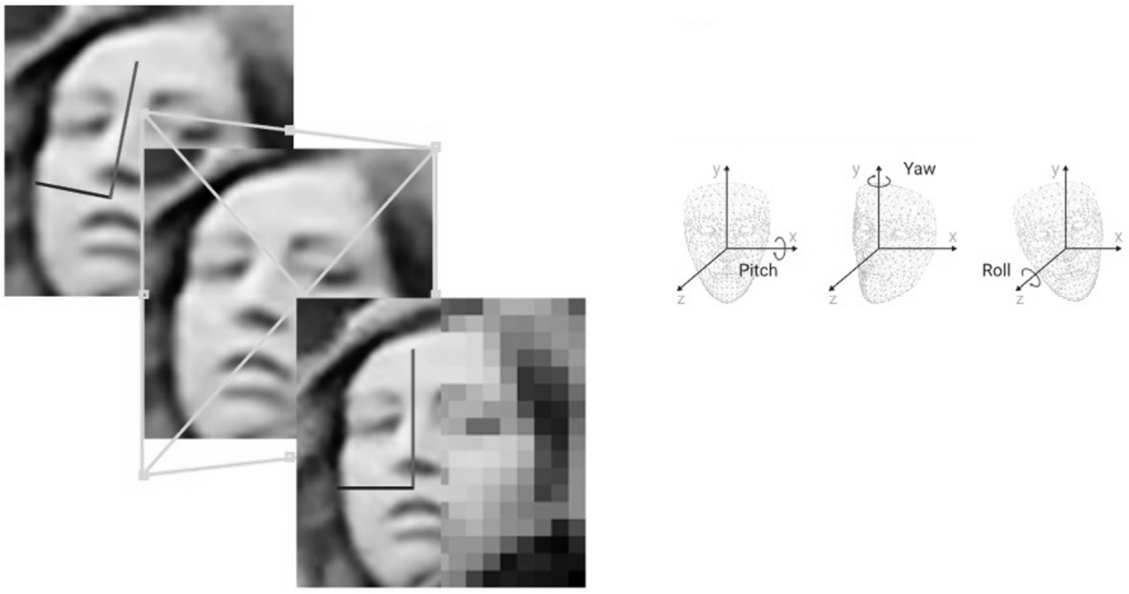


Рис. 4. Исправление визуальных искажений

NtechLab использует в своих продуктах собственную технологию детектирования Liveness, который не требует дополнительных действий от посетителей (улыбнуться, моргнуть или иначе взаимодействовать с системой идентификации) и работает с уже имеющимся оборудованием (не требуется устанавливать специализированные устройства). Алгоритм NtechLab также определяет силуэт и отслеживает его путь при прохождении мимо камеры.

Главные задачи, которые эффективно решает распознавание по силуэту, – это мгновенный и точный подсчет огромного количества людей в видеопотоке, а также межкамерное (в пространстве между камерами) отслеживание перемещения силуэтов.

Подобные технологии распознавания лиц в толпе могут быть использованы органами внутренних дел при отслеживании или отождествлении конкретного лица или группы лиц в процессе соответствующих оперативно-розыскных мероприятий, в особенности проводимых по факту деяний, содержащих признаки преступлений против общественной безопасности.

Поисковая система «СЕУС»

Поисковая система «СЕУС» позволяет решать задачи, связанные с поиском, мониторингом и анализом информации, размещенной в социальных сетях, а именно выполнять мониторинг

информации (исследование) в различных разрезах при помощи одновременного поиска по списку слов и словосочетаний – лингвистическому словарю терминов [12, 13].

«СЕУС» может быть использована для своевременного выявления фактов и источников размещения информационных материалов соответствующей тематической направленности с целью предотвращения их дальнейшего распространения. Данное программное обеспечение осуществляет поиск информации в следующих социальных сетях: «ВКонтакте», Facebook, Instagram[1], Twitter[2], «Одноклассники». К достоинствам рассматриваемого программного обеспечения можно отнести поддержку работы в нескольких социальных сетях и большое количество фильтров, по которым производится поиск информации. Программное обеспечение «СЕУС» успешно используется правоохранительными органами в 20 регионах России.

Поисковая система «СЕУС» предоставляет пользователям следующие функциональные возможности:

– полнотекстовый поиск и мониторинг информации без дополнительной настройки со стороны оператора с получением результата в течение трех минут (зависит от характеристик канала связи с сервером);

– набор фильтров для поиска информации и несколько видов мониторинга пространства социальной сети при помощи лингвистических словарей;

– поддержка различных языков поиска и мониторинга информации, включая арабский;

– полное географическое покрытие информационного пространства на территории Российской Федерации;

– поиск профилей пользователей по различным параметрам, в том числе по неполным данным;

– экспорт информации в привычные офисные форматы и визуализация результатов работы на нескольких видах административных карт территорий регионов страны;

– коллекции контента.

---

[1] Здесь и далее: деятельность социальных сетей Instagram и Facebook, принадлежащих компании Meta Platforms Inc., признана экстремистской и запрещена на территории России.

[2] Здесь и далее: Twitter заблокирован в России по требованию Генпрокуратуры за распространение незаконной информации.

Программный комплекс «Поисковая система “СЕУС”» (рис. 5) может использоваться для решения задач оперативных подразделений, связанных с мониторингом и анализом информационной обстановки в открытом пространстве социальных медиа, поиском противоправного и деструктивного контента, а также цифровых следов лиц, его распространяющих.

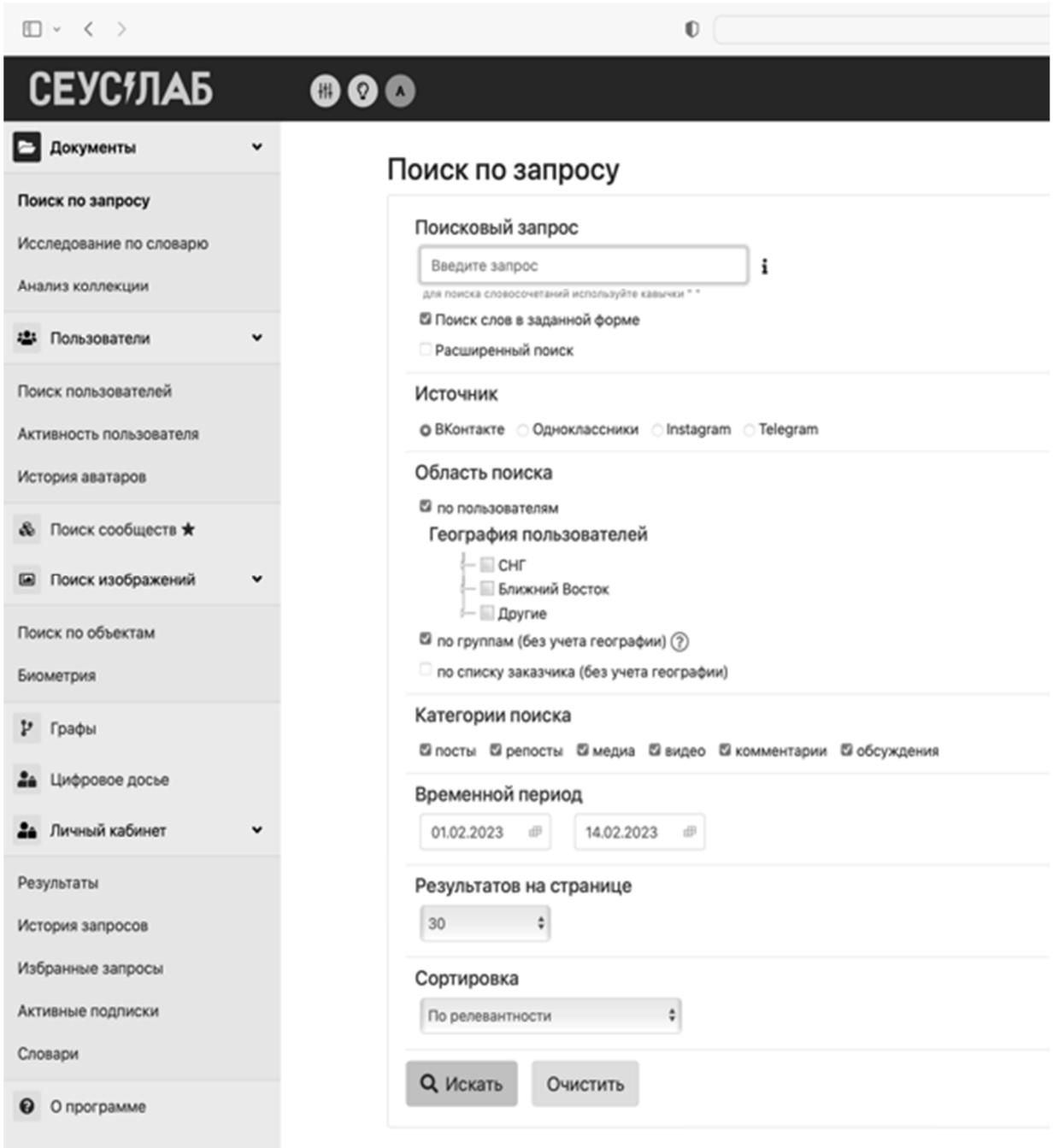


Рис. 5. Главное окно поисковой системы «СЕУС»

Программный комплекс «Поисковая система “СЕУС”» позволяет получать информацию без обращения к администрации социальных медиа и предоставляет пользователям следующие возможности:

– поиск контента на любом языке мира (включая Арабский) в течение трех минут (зависит от характеристик канала связи с сервером);

– поиск профилей пользователей по анкетным (в том числе неполным) и биометрическим данным;

– поиск изображений, содержащих символику террористических, экстремистских организаций, различные виды оружия и получение информации об их авторах;

– получение удаленных или измененных цифровых следов пользователей социальных сетей и информации об их сетевой активности: тексты удаленных материалов, изменения анкетных данных, история аватаров;

– получение информации о связях профилей и их анализ при помощи графовых технологий.

Все полученные данные хранятся в защищенном центре (хранения и) обработки данных, а программный комплекс «Поисковая система “СЕУС”» предоставляется пользователю в формате веб-сервиса и не требует установки на служебные ЭВМ.

Используемая в работе методика выявления и анализа элементов «цифрового портрета потенциального объекта интереса» определяет блоки задач, которые можно решать при помощи программного комплекса «Поисковая система “СЕУС”» (рис. 6).

Рис. 6. Возможности поисковой системы «СЕУС»

Рассмотрим пример работы поисковой системы «СЕУС» при выявлении в сети Интернет лиц, осуществляющих содействие террористической деятельности (ст. 205.1 УК РФ).

Фабула: различного рода благотворительные организации и фонды занимаются сбором пожертвований и оперируют собранными средствами в дальнейшем. Часть из этих средств может использоваться для финансирования террористической деятельности.

Задача:

– выявить в пространстве социальной сети «ВКонтакте» профили пользователей, публикующих призывы к осуществлению финансирования террористической деятельности;

– получить количественное представление о зональном распределении значений (где «значением» выступает пост (репост) с признаками финансирования террористической деятельности) путем формирования административно-территориальной карты;

– выделить пользователей конкретной административной единицы;

– сформировать набор отождествляющих и характеризующих признаков выявленных пользователей.

Исходные данные: текстовый запрос, состоящий из двух словоформ – *«Киви-кошелек»* и *«джихад»,* с периодом публикации с 31.01.2013 по 31.12.2015 (география поиска: Приволжский федеральный округ). Категория поиска: пост (репост).

Результат: с применением функционального блока «Поиск по запросу» поисковой системы «СЕУС» получена выборка данных, состоящая из 20 сообщений, в которых содержатся ссылки на посты и репосты, соответствующие исходным данным; результаты поиска визуализированы на интерактивной карте административно-территориального деления – Приволжский федеральный округ (табл. 1).

Таблица 1

Распределение полученных значений (Приволжский федеральный округ)

Дата начала	Дата окончания	Регион	Метрика	Количество пользователей
31.01.2013	31.12.2015	Республика Башкортостан	6	5 413 061
31.01.2013	31.12.2015	Марий Эл	0	690 059
31.01.2013	31.12.2015	Мордовия	0	663 745
31.01.2013	31.12 2015	Пензенская область	0	1 185 996
31.01.2013	31.12.2015	Самарская область	0	4 271 470
31.01.2013	31.12.2015	Саратовская область	1	2 246 182
31.01.2013	31.12.2015	Республика Татарстан	9	5 754 973
31.01.2013	31.12.2015	Удмуртская Республика	2	1 637 959
31.01.2013	31.12.2015	Ульяновская область	1	1 184 478
31.01.2013	31.12.2015	Чувашская республика	0	1 309 095
31.01.2013	31.12.2015	Кировская область	0	1 493 309
31.01.2013	31.12.2015	Нижегородская область	0	3 910 281
31.01.2013	31.12.2015	Оренбургская область	1	2 004 756
31.01.2013	31.12.2015	Пермский край	0	3 828 076

Продемонстрируем работу функционального блока «Поиск по запросу» на примере одного из найденных поисковой системой «СЕУС» результатов (продолжим на примере выявленных профилей пользователей Республики Татарстан).

Контент найденного поста, содержащий такие поисковые слова, как *«Киви-кошелек»* и *«джихад»,* представлен в табл. 2 и 3. Найденные слова выделены в примере *курсивом.*

Таблица 2

Примеры сообщений о финансировании терроризма

Тип	пост
Источник	https://vk.com/id232945141
Место размещения	ВКонтакте
Содержание документа	(15.04.2014 14:44:40)
«Ассаламу алейкум дорогие братья и сестры АлхамдулиЛлях, слава Аллаху который собрал нас на этой благославеной земле Шама и позволил нам работать на его пути и возвыщать Его слово. Очень многие братья каждым днем отдают свои души на пути Аллаха, они все благи этого мира меняют с удовольствием на вечную жизнь в раю инщааЛлах. Оставить своих детей и близких и выйти на этот путь это не простое дело. У тех братьев кто ушел инщааЛлах к Аллаху есть у многих семьи на этой земле и они все еще тут, АлхамдулиЛлях не уезжают кафирским землям обратно – ведь самое благославеное земля это Шам инщааЛлах. У джамаата не всегда получается полностью обеспечивать и помогать, но АлхамдулиЛлях как может Амиры АлхамдулиЛлях справедливо помогают семьям шахидов. Есть сестры жены шахидов, их маленькие инщааЛлах муджахиды и муджахидки любимцы Аллаха инщааЛлах. Братья и сестры, какое еще благое дело лучше чем *джихад* найдете в исламе? Давайте бисмиЛлях все вместе сделаем благое дело инщаЛлах. Пророк С.А.В сказал: «Ман такаффала аль йатима кунту ана ва хува филь джаннати кахатейин джамъа байнал усба аъйн». Кто будет обеспечивать сироту, я и он будем в раю вместе (рядом, т. е. показал свой указательный палец и средний соеденив их). Имам Бухари, сахих хадис. Пророк С.А.В сказал: «Ассаи алал армалати вал аъйтам кал муджахиди фисабилиЛлях Кто смотрит за семью муджахида (вдова шахида, сирота шахида)». Он поистине как Муджахид на пути Аллаха фисабилиЛлях. Я ВаЛлахи хочу посмотреть на то, что мы сможем сделать на пути Аллаха, ВаЛлахи давайте уже просыпаться и смотреть на вещи реальностью, мы все знаем что все что мы копили и зарабатывали останется в этой дунье и знаем что цена рая очень дорого, получить довольствие Аллаха не просто. Ради Аллаха прощу вас, делайте репосты распространите это сбор везде где можно, ВаЛлахи если есть мискин и муджахид первым надо помочь муджахиду, так давайте вместе все поможем семьям шахидов и их детям – не важно с аакого джамаата они и какого национвльности, я помогу тем кому нужна помощь и инщааЛлах ваш амана до пейса доставлю нуждающимся. ВаЛлахи, это благое дело пусть распространится везде, и это благое дело желайте рекомендуйте всем своим близким и друзьям – купите себе биизниЛлях	

рай братья и сестры мои. ВаЛлахи может я сегодня есть завтра нет, я отказался от благи этого мира и ВаЛлахи я до последнего вздоха хочу больше и больше пользы принести для религии Ислам для джихада. До следующего понедельника инщааЛлах это сбор будет в интернете, и я хочу узнать насколько мои братья и сестры коьорые не находятся тут хотят шариат и халифат, насколько они любят своих братьев и будут поддерживать муджахидом которые инщааЛлах воюют на пути Аллаха за шариат. Поистине помогая муджахидам вы делаете *джихад* на пути Аллаха и свою награду в увеличенном виде получите у Аллаха. Даже если каждый из нас по 100 рублей, ВаЛлахи это уже будет огромные деньги и представляете какую помощь можно сделать ? Нет, не сможете представить, это для них инщааЛлах будет праздник лучший праздник, они будут чувствоват чувствоват поддержку вашу они будут чувствовать вашу любовь, ведь эти шахиды пали на пути Аллаха что бы установить закон Аллаха на земле и освободить от притеснение на этой земле нас, освободить от кафиров тагутов. *Киви кошелек*: +79175485717 отправляйте деньги с комментарием для семья шахидов. Есть еще виза карта, а тем кто в европе есть вестерн юнион. ВаЛлахи, Аллах и вы будете знать о вашем благом дело и аджр будет очень огромный инщааЛлах, я лично буду свидетельствовать в судный день что вы помогли мискинам и вы были фисабилиЛлях на Его пути и что юы Аллах защитил вас от огня ада инщааЛлах. Пропрок С.А.В сказал: «Иттаку наро ва лав бишикки тамр». Защищайтесь от огня ада, хотя половинкой финика. Имам Бухари. Сахих хадис. ДжазакаЛлаху хайран».

Результаты ответа на запрос содержат информацию, которая подлежит дальнейшей обработке, а именно – полученные данные способствуют выявлению характеризующих и отождествляющих признаков пользователя с id232945141: используемая в постах и репостах лексика (табл. 3).

На текущий момент пользователь с id232945141 заблокирован. Использование функционального блока «Активность пользователя» поисковой системы «СЕУС» позволило получить выборку данных, содержащих посты, репосты, комментарии (всего 248 позиций) пользователя с id232945141.

Выборка данных включает в себя всю активность пользователя в социальной сети «ВКонтакте» с даты регистрации – 29.11.2013 до даты блокировки – 03.08.2015.

Таблица 3

Записи в социальной сети «ВКонтакте»

15.03.2014 01:53:02 yaa robbi
«Асселем, алейкум. Вот *киви кошелек* 917 548-57-17 (на это же счет можно пополнять и с Казахстана тенге, и с Украины гривни – с терминалов Qiwi), одна сестра БисмиЛлях сделала кошелек. Это тем братьям и сестрам которые делают *джихад* на пути Аллаха своим имуществом. Вашими деньгами инщааЛлах помогу женам шахидов и раненым братьям, или тем кто нуждается. Не будьте равнодушным, тут есть много мусульман которые нуждаются в помощи Аллаха и его искренних рабов которые делают *джихад* своим имуществом. За 100 рублей которые вы отдадите тут можно купить продукт на день то есть один день проживет сытым один человек. инщааЛлах. Чтобы вы не делали на пути Аллаха вы награду получите в день воздаяние. О те, которые уверовали! Если вы поможете аллаху, то и Он поможет вам и утвердит ваши стопы. (47/7) Притчей о тех, кто расходует свое имущество на пути Аллаха, является притча о зерне, из которого выросло семь колосьев,и в каждом колосе – по сто зерен. Аллах увеличивает награду, кому пожелает (сура «Корова», аят 261). Сделайте репост, донесите это инфо тем кто хотят помочь, работайте на пути Аллаха поддержите нас а Аллах поддержит вас. Я не джамаат и я не делаю сбор для джамаата, я один человек и этим инщааЛлах благим делом занимаюсь один. Отчет поступления денег на кошелек: http://vk.com/topic-66454641 Реквизиты visa карты: 4890 ****».

Отождествляющие признаки пользователя с id232945141: анкетные данные, аватар, номера телефонов (рис. 7).

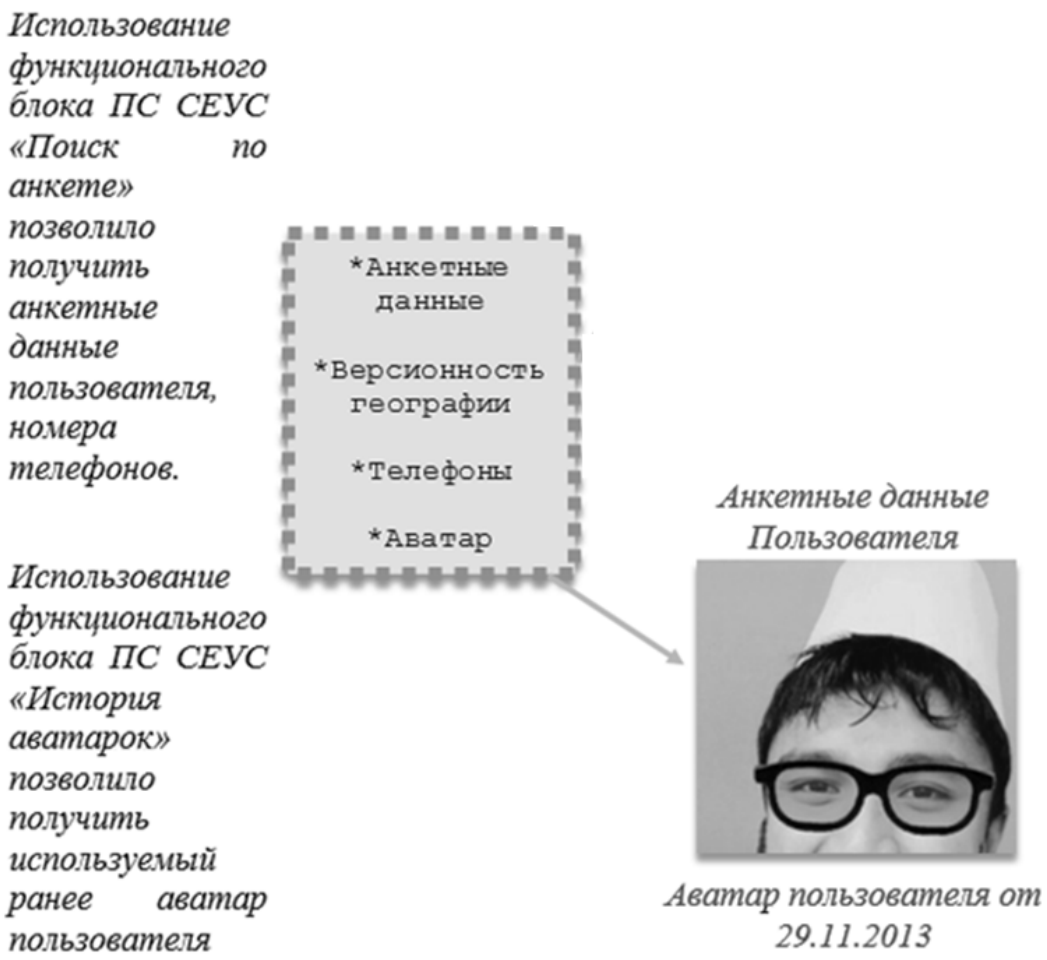


Рис. 7. Отождествляющие признаки пользователя с id232945141

Различные версии местоположения («версионность», термин «СЕУС») пользователя доступны в хранилище поисковой системы «СЕУС» (рис. 8).

Версионность параметра "География пользователя"

Пользователь

#	География пользователя	Дата начала	Дата изменения
2	Ташкент (Ташкентская, Ташкентская, Узбекистан)	25 марта 2018	актуально
1	Казань (Республика Татарстан, Российская Федерация)		25 марта 2018

Рис. 8. Версионность географии пользователя с id232945141

На выявление и последующее отождествление пяти профилей пользователей социальной сети «ВКонтакте», разместивших

посты о финансировании террористической деятельности (в данном посте усматриваются признаки преступления, предусмотренного ст. 205.1 УК РФ), было затрачено около 30 минут.

Автоматизированная система круглосуточного мониторинга и сбора данных «Демон Лапласа»

«Демон Лапласа» – это автоматизированная система круглосуточного мониторинга и сбора данных из сети Интернет, позволяющая получать и анализировать широкий спектр информации из социальных сетей Facebook, «ВКонтакте», «Одноклассники» и Instagram, микроблогов Twitter, онлайн-СМИ, а также из персональных блогов «Живого журнала» и мессенджера «Телеграм» [16].

К перечню заявленных разработчиками возможностей программного обеспечения относятся следующие модули.

1. Мониторинг бренда. Модуль осуществляет мониторинг онлайн-СМИ и их страниц в социальных сетях. Поиск ключевых фраз в сообществах регионального сегмента.

Программный комплекс «Демон Лапласа» позволяет автоматизировать процесс получения информации из социальных сетей и онлайн-СМИ, связанных с упоминаниями брендов, и показывать на мониторе сотрудника ОВД полученную информацию как в разрезе каждой социальной сети отдельно, так и в каждом отдельно взятом регионе. Уход от сплошного мониторинга онлайн-СМИ к региональному, круглосуточному сбору данных в режиме реального времени о ключевых факторах цели и ее упоминаний дает возможность прогнозировать действия отдельных лиц или организаций в каждом конкретном регионе или в стране в целом. Распространение такого анализа на все социальные сети увеличивает результативность работы сотрудника ОВД, осуществляющего поисковый запрос. Данный модуль программного обеспечения позволяет производить сбор и вывод данных раздельно по каждой социальной сети, настраивать фильтрацию спама, получать информацию об авторах, производить поиск лидеров мнений, визуализировать результаты в виде графиков и диаграмм, получать ретроспективу и выводы публикаций по дате, экспортировать данные с возможностью редактирования.

2. Конкурентная разведка. Модуль, позволяющий автоматически фиксировать рост числа подписчиков в сообществах, интересующих сотрудника ОВД.

Модуль позволяет в автоматизированном режиме производить анализ сообществ в социальных сетях и публичных страниц интересующих лиц. Присутствуют возможности ведения учета, сортировки подписчиков интересующих сообществ, генерации диаграмм, а также экспорта полученных данных. Сравнительный анализ прироста участников в созданных сотрудником ОВД кластерах дает возможность фиксировать скачки прироста аудитории в тех или иных тематических сообществах за определенный период времени. Анализ таких скачков помогает выявить причины повышенного внимания пользователей социальных сетей к деструктивным сообществам и группам.

3. Сетевая визуализация. Модуль предназначен для поиска лидеров мнений, отслеживания их активности, систематизации, хранения и экспорта публикаций.

Рассматриваемый модуль позволяет осуществлять круглосуточный мониторинг сетевых сообществ; находить лидеров мнений, оказывающих на аудиторию социальных сетей наибольшее влияние; производить фиксацию таких параметров, как количество публикаций и число комментариев; дает возможность выявлять среди общей массы аккаунтов те, которые пользуются наибольшей поддержкой своих подписчиков и формируют отношение аудитории в том или ином сообществе. Ввод в систему интересующих сотрудника ОВД маркеров позволяет фиксировать начало информационных атак и оперативно находить их источники. В программном комплексе предусмотрена возможность оповещения по средствам отправки предупреждающих сообщений на электронную почту и СМС на смартфон сотрудника ОВД в случае появления в сети или в узко заданном ее сегменте сообщений определенной тематики. Все публикации и комментарии к постам лидеров мнений автоматически сохраняются в базе данных. По запросу сотрудника ОВД система способна строить сетевые графы, отражающие связи пользователей как по принципу взаимной дружбы, так и по комментированию публикаций.

4. Экстремизм и терроризм. Модуль, позволяющий проводить автоматизированный поиск распространителей экстремистского контента и пропаганды исламистских организаций.

Модуль позволяет настроить автоматизированный поиск экстремистского контента, выдает по запросу сотрудника ОВД список аккаунтов, распространяющих запрещенные публикации, аудио- и видеоконтент, отсеивая пользователей из всех прочих городов, кроме того, который интересует сотрудника ОВД. Результаты поиска выдаются в виде таблицы, содержащей информацию о владельце аккаунта с запрещенными роликами, его контактные данные и личные фотографии.

5. Прогнозирование. Кластерный анализ целевых сообществ. Сбор статистических данных. Визуализация сетевых изменений.

Этот программный модуль позволяет производить сегментированный по географическому признаку анализ религиозных настроений и межнациональных отношений, дает возможность находить и локализовывать источники распространения информации, реагируя на катализаторы негативной активности, ведущей к межнациональным и межконфессиональным конфликтам. Применение кластерного анализа в оперативном мониторинге помогает оценивать степень активности в сообществах профильных тематик. Так, можно разделить сообщества на националистические и исламистские, либеральные и леворадикальные, замеряя активность не только в той или иной группе, но и в кластере таких групп, сравнивая историю и делая прогнозы. Алгоритм позволяет фиксировать волнующие аудиторию темы медийного пространства и по заявлению разработчиков успешно применяется для прогнозирования межнациональных и межконфессиональных конфликтов.

Платформа «Крибрум»

Акционерное общество «Крибрум» – исследовательская и технологическая компания, основанная в 2010 г. Организация является разработчиком одноименной платформы для мониторинга и анализа данных из различных источников в Интернете [21].

Платформа «Крибрум» обеспечивает постоянный мониторинг, сбор и возможность анализа данных социальных медиа в режиме, близком к реальному времени, 60% всего потока собирается за время от 15 минут, а весь поток – в течение 3–5 часов. Все собранные данные с 2014 г. хранятся на собственных серверах, которые располагаются на территории Российской Федерации. Общий объем всех данных составляет более 5 петабайт. Ежедневно платформа собирает порядка 140 млн текстовых сообщений, 40 млн изображений, 500 млн действий аккаунтов социальных сетей. Информация собирается из 70 тыс. источников: СМИ, форумы, блоги, информационные порталы, социальные сети (Facebook, Instagram, Twitter, TikTok, «ВКонтакте», «Одноклассники»), видеохостинг YouTube, телеграм-каналы, рекрутинговые платформы hh.ru и superjob.ru, некоторые популярные форумы в сегменте DarkNet (рис. 9).

Рис. 9. Характеристика сбора и собираемые источники сообщений

Одно из приоритетных направлений развития платформы – ввод новых языков мониторинга данных. На сегодня поддерживается сбор и анализ на 23 языках: русский, английский, арабский, китайский, литовский, латышский, казахский, киргизский, молдавский, узбекский, азербайджанский, украинский, белорусский, грузинский, армянский, эстонский, таджикский, туркменский, болгарский, польский, венгерский, чешский, словацкий. Автоматически проводится определение текста в изображениях и его распознавание. Это не единственный вид работ с изображе-

ниями – активно развиваются собственные алгоритмы машинного обучения для распознавания лиц и объектов (в основном символики запрещенных на территории Российской Федерации организаций).

В компании также работает собственный аналитический центр, куда входят математики, алгоритмисты, аналитики, специалисты по прикладной лингвистике, лингвисты, политологи, социологи и поведенческие психологи. Эксперты проводят различные медиаисследования и медиаизмерения, разрабатывают собственные прогностические методы, анализируют социальные, экономические и политические процессы, проводят исследования по направлению поведенческой психологии, расследования по открытым данным (OSINT).

Система «Крибрум.Объекты» предназначена для постоянного оперативного мониторинга и сбора текстовых сообщений и изображений с текстом в социальных медиа, куда входят популярные социальные сети, форумы, онлайн-СМИ и прочие интернет-источники.

Концепция системы подразумевает следующий подход: «Крибрумом» для клиента создается специальный проект, внутри которого сотрудник ОВД создает специальные конструкции, называемые объектами, в которые добавляет поисковые запросы и сохраняет. С момента создания объекта в проект непрерывно начинают загружаться все сообщения, которые соответствуют поисковым запросам. Алгоритм настройки работы прост, достаточно правильно и исчерпывающе обозначить поисковыми запросами то, что необходимо собирать. Система обеспечивает возможность пользователю создавать сложные поисковые запросы, благодаря которым осуществляется полнотекстовый поиск сообщений с учетом морфологии русского языка (нахождение указанных слов в любых словоформах), а также с учетом опечаток и различных вариантов написания слов. Это дает возможность описать запросами практически что угодно: упоминание персоны (ведомства, компании), сообщения с угрозами (призывами) и признаками экстремисткой направленности, сообщения по тематике наркоторговли, сообщения с упоминаниями запрещенных на территории Российской Федерации организаций и т. д.

Настроив интересующие объекты мониторинга, можно оперативно получать сообщения со всех платформ, с которых осуществляется сбор данных. Немаловажной особенностью системы является возможность запустить загрузку в проект ретроспективных данных по объекту мониторинга, что даст возможность проанализировать весь объем информации с 2014 г.

«Крибрум.Объекты» автоматически определяет эмоциональную окраску высказывания относительно объектов мониторинга (тональность), автоматически распределяет публикации по тематикам, устанавливает географию сообщения, распознает первоисточники и дубли, рассчитывает самых активных и популярных авторов и т. д.

Совокупность всех функций дает возможность фильтровать и сортировать практически как угодно весь собранный массив данных: по ключевым словам, дате публикации, источнику, автору, географии, тональности и прочему.

Система «Крибрум.Зеркало» предназначена для автоматизированного анализа действий аккаунтов, нахождения связей между аккаунтами, оперативного выявления признаков риска в поведении пользователей социальных медиа.

Система собирает данные только из открытых аккаунтов. При этом благодаря сбору информации из сотен миллионов открытых профилей различных социальных сетей появляется возможность анализа действий любого искомого аккаунта (посты, лайки, комментарии и т. п.) в случае их взаимодействия.

Возможен также анализ действий уже удаленных аккаунтов, так как данные уже были загружены в систему.

«Крибрум.Зеркало» дает возможность изучить все действия аккаунта. Их количественные характеристики визуализируются на графиках и диаграммах.

Еще один немаловажный функционал в «Крибрум.Зеркало» – это так называемые правила (рис. 10). Они представляют собой сценарии, которые сотрудник ОВД настраивает для анализа аккаунтов.

Допустим, необходимо, не просматривая все реакции аккаунта, сразу оценить, на какие темы с него писали. Для этого формируются лингвистические запросы, подобные тем, которые формулируются в «Крибрум.Объектах», например: «интерес к

деструктивным движениям», «интерес к наркотическим веществам», «интерес к изготовлению оружия» и т. п. Благодаря лингвистам и экспертам компании в области исследования деструктивных течений, поведенческим психологам мы сформировали и постоянно обогащаем собственный набор таких правил. Такой набор позволяет автоматически сформировать портрет аккаунта, который можно выгрузить из системы в форме отчета.

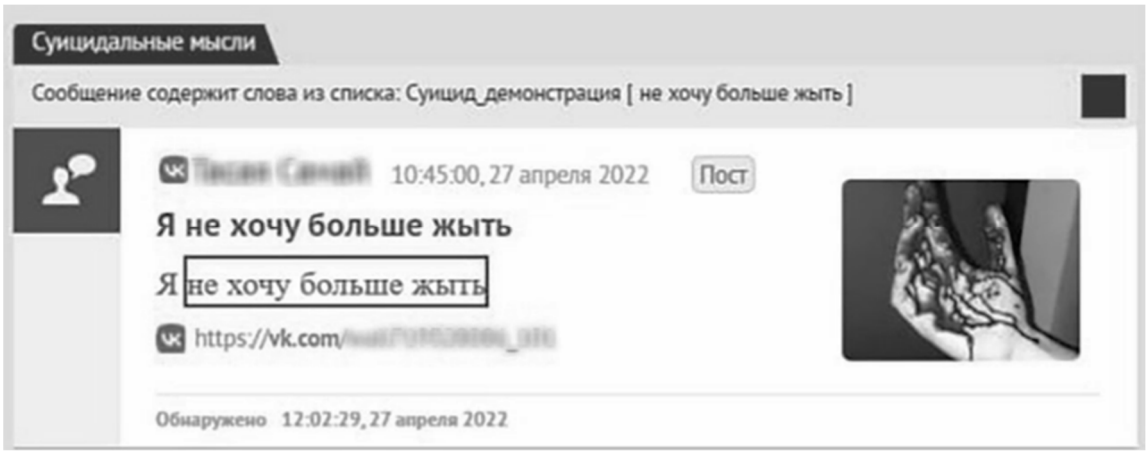


Рис. 10. Пример срабатывания правил в системе «Крибрум.Зеркало»

Возможности системы «Крибрум.Зеркало» эффективны в сфере информационной и общественной безопасности, при проведении социологического анализа физических лиц.

Система «Крибрум.Поиск» предназначена для оперативного поиска упоминаний в текстовых сообщениях. Поиск ведется с учетом морфологии русского языка (нахождение указанных слов в любых словоформах) в сообщениях, опубликованных за последние шесть месяцев. Поиск осуществляется по всем источникам, по которым поддерживается сбор.

Система представляет собой поисковую машину, подобную «Яндекс», но осуществляющую поиск по данным, собранным «Крибрум». Как известно, популярные поисковые машины индексируют только малую часть социальных сетей, в основном это анкетные данные, некоторые публикации. При этом при помощи «Крибрум.Поиск» можно быстро провести поиск по неиндексируемому пространству другими поисковыми машинами, например найти комментарии пользователей в социальных сетях, телеграм-каналах или на YouTube.

Кроме того, система позволяет представить в формате графика количество упоминаний поискового запроса, что дает возможность оценить, в какие периоды времени наиболее популярным был его поисковый запрос.

Система «Крибрум.Сигнал» предназначена для графического анализа распространения информации в социальных сетях (рис. 11).

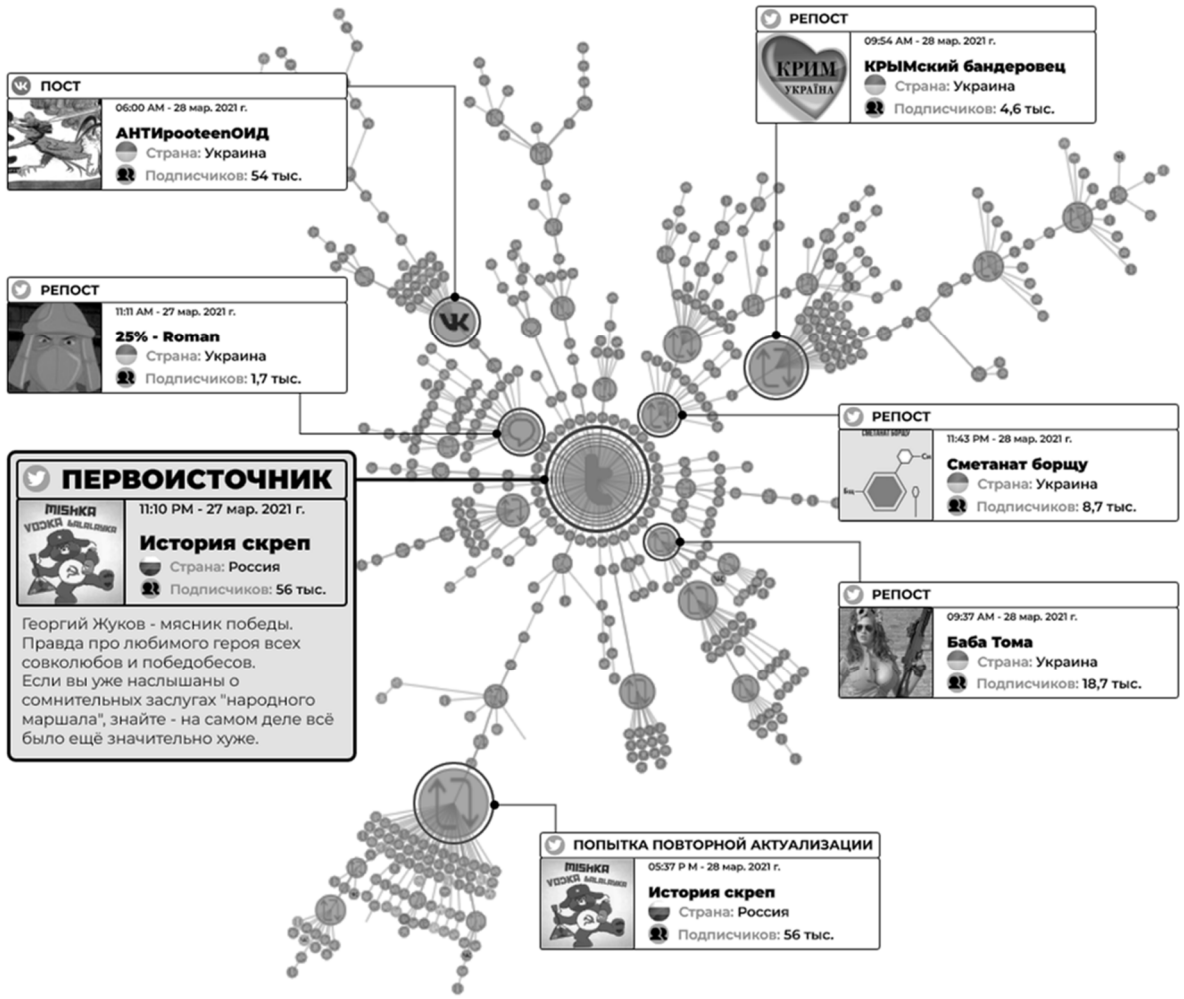


Рис. 11. Пример анализа характера распространения информации в системе «Крибрум.Сигнал»

Функциональные возможности системы обеспечивают пользователя возможностью оперативно отследить источники и пути распространения информации, определить естественный или искусственный характер ее распространения.

Информационно-аналитическая система «Семантический архив»

Информационно-аналитическая система (АИС) «Семантический архив» разработана компанией «Аналитические бизнес решения» [25] и предназначена для автоматизации деятельности соответствующих служб различных организаций и государственных структур, в том числе МВД России.

Система позволяет организовывать сбор текстовой информации из открытых источников (электронные СМИ, аналитические отчеты экспертов), осуществлять их обработку, эффективное хранение, проведение анализа и генерацию. Информационно-аналитическая система «Семантический архив» предоставляет сотруднику ОВД возможность создавать формальные досье на различные объекты мониторинга – персоны, компании, государственные структуры, а также хранить описания их взаимоотношений и событий, происходивших с ними. Часть таких описаний может иметь ссылки на материалы, в которых и упоминалось о конкретных фактах, найденных в сети Интернет. Несмотря на название АИС, архивных копий информации на сайте АИС найти не удалось.

2.3. Программное обеспечение для поиска информации по архивным данным интернет-ресурсов

Архив профилей VK.watch

VK.watch – история профилей в социальной сети «ВКонтакте» – представляет собой сервис, осуществляющий поиск людей по уникальному ID (ID – часть английского слова identifier, идентификатор или имя, номер, набор цифр, букв) либо по последнему никнейму (псевдоним, используемый пользователем) в социальной сети «ВКонтакте». Программная система обладает большим архивом исторических данных, таких как фотографии, комментарии к различным фотографиям, видео, посты, списки друзей, изменения профилей пользователей. Процесс использования данного инструмента осуществляется без авторизации в социальной сети «ВКонтакте» [14].

Сервис выводит всю открытую и необходимую информацию о профиле пользователя и структурированно отображает ее, что недоступно при использовании в целях сбора информации непосредственно социальной сети «ВКонтакте».

Алгоритм применения данного инструмента представляет собой простую последовательность действий.

1. После перехода на сайт необходимо ввести уникальный ID или последний никнейм, затем нажать на окно, соответствующее поиску.

2. Осуществлять поиск рекомендуется по цифровому ID пользователя по причине возможности изменения никнеймов и их непостоянства.

По данным самого сервиса, в его архиве содержится информация приблизительно о 355 млн пользователей, количество фотографий доходит до 975 млн.

Сервис позволяет просмотреть основную информацию о пользователе, такую как имя, фотографии, группы, а также комментарии пользователей, списки друзей и изменения профилей.

Основная масса данных сервиса сформирована в 2016 г., и в августе 2018 г. VK.watch запущен с данной базой на самоокупаемой основе. В 2019 г. появилась возможность находить людей по лицам, как у закрывшегося FindFace, – достаточно загрузить фотографию.

Кроме того, сервис VK.watch позволяет найти информацию о друзьях и подписчиках пользователя, а также о сообществах, в которых он состоит.

Одним из главных преимуществ сайта https://vk.watch является его удобный и простой интерфейс. Пользователи могут легко и быстро найти нужную информацию о профиле, не тратя много времени на поиск. Кроме того, сервис не требует регистрации в «ВКонтакте», что делает его еще более удобным в использовании.

VK.Watch имеет свои недостатки, которые следует учитывать при использовании этого инструмента.

1. Недостаточная актуальность информации: в базе данных VK.Watch содержится информация, которая может быть устаревшей или неактуальной. Это связано с тем, что пользователи социальной сети могут изменять свои профили, удалять фотогра-

фии или добавлять новые. Поэтому результаты поиска на VK.Watch могут не соответствовать действительности.

2. Ограниченный функционал: VK.Watch предназначен только для поиска профилей в социальной сети «ВКонтакте», сформированных до 2019 г.

VK.Watch может быть полезным инструментом в правоохранительной деятельности, так как он содержит большое количество информации о старых пользователях социальной сети «ВКонтакте», что говорит о достоверности размещаемых данных и более точной идентификации лица.

Например, при расследовании уголовных дел сотрудники правоохранительных органов могут использовать этот сервис для выявления связей между подозреваемыми, их друзьями и знакомыми, а также для поиска фотографий, позволяющих идентифицировать интересующих лиц, или подтверждения факта события преступления.

Сервис по поиску архивных копий сайтов Web archive

В 1996 г. в США был создан сайт archive.org, который представлял собой сервис, осуществляющий сбор и хранение всей публичной информации, размещенной в сети Интернет, в некоммерческих целях. Российским аналогом является сайт web-archive.ru [19]. С его помощью можно получить не только информацию из прошлого, сохраненные копии сайтов разных лет, но и метаданные. Иными словами, веб-архив отображает своеобразный слепок Интернета в определенный период времени. Сервис находится в свободном доступе, а в результатах поиска не отображаются лишь те сайты, в настройках которых установлен запрет на сохранение размещенной на них информации.

Формирование базы данных веб-архива происходит с помощью программного обеспечения, осуществляющего многократное посещение веб-сайтов с определенной частотой. Сервис может оказаться полезен для поиска утраченной информации об определенном лице, например, путем введения в графу для поиска ссылки на аккаунт профиля в социальной сети «ВКонтакте». В результате поиска информации в веб-архиве могут быть найдены

удаленные фотографии, посты, комментарии и видео, документы и другая недоступная на актуальных страницах информация.

Для работы с сервисом в строку поиска необходимо ввести ссылку на сайт, архивную версию которого необходимо просмотреть. Вверху интерфейса располагается временная шкала, с помощью которой можно перемещаться по копиям сайта в различное время.

2.4. Программное обеспечение для поиска информации в мессенджерах

В современном обществе большое распространение получили мессенджеры, устанавливаемые на смартфоны для обмена информацией между людьми, функционирующие с использованием телекоммуникационных технологий и Интернета. Наиболее популярные из них: WhatsApp, Viber, «Телеграм», ICQ и др. Умение осуществлять поиск в мессенджерах различных сведений также является важной задачей для сотрудника ОВД. Далее на примере одной из популярных платформ «Глаз Бога» показана возможность поиска большого количества сведений о конкретном человеке.

Платформа «Глаз Бога»[1] (Eye Of God) представляет собой разработанную программу в виде специального аккаунта кроссплатформенного мессенджера «Телеграм», которая выполняет различные действия по заранее установленным командам [15]. Такие аккаунты играют роль интерфейса определенного сервиса, который работает на удаленном сервере.

Основные преимущества ботов состоят в следующем:

– высокая скорость обработки получаемой информации;

– удобный и понятный для обычного пользователя интерфейс;

– отсутствие потребности в регистрации на специализированных сайтах;

[1] Таганский суд Москвы признал работу телеграм-бота незаконной и нарушающей права граждан на неприкосновенность частной жизни, личную и семейную тайну.

– большое количество редкой и качественной информации.

Бот платформы «Глаз Бога» представляет широкий функционал по поиску информации о конкретном человеке.

Поиск может осуществляться по большому количеству параметров:

– фото лица;

– фамилия, имя, отчество человека;

– номер телефона;

– электронная почта;

– номер машины;

– номер банковской карты;

– возможный пароль от определенного сервиса (в таком случае строка поиска будет иметь следующий вид: «/pas» + «пароль»);

– ИНН по запросу вида «/inn» + «номер».

Результатом поиска могут быть данные самого различного характера: возможный профиль пользователя социальной сети, номер телефона, пароли, оказавшиеся в открытом доступе, предполагаемые варианты записи данного контакта у других людей, социальные сети, привязанные к электронной почте, возможные адреса, в случае если лицо оформляло доставку по номеру из интернет-магазинов.

Важной особенностью является возможность поиска информации о юридических лицах с помощью запроса следующего вида: «/company» + «название организации». По данным самого проекта, в базах содержится примерно 3,2 млн адресов электронной почты и 25,2 млн телефонных номеров.

Технология имеет ряд значительных преимуществ:

– разные параметры поиска;

– обширная база данных;

– оперативная служба поддержки;

– регулярные обновления;

– понятный и удобный интерфейс;

– сохранение истории всех запросов, возможность ее просмотра в любой момент времени;

– наличие дополнительной информации, отзывов пользователей, тематических статей.

Для поиска информации «Глаз Бога» использует различные открытые источники:

1) социальные сети (Facebook, Twitter, Instagram, YouTube, Reddit, LinkedIn, «ВКонтакте», TikTok, Badoo, Tinder, Getcontact);

2) мессенджеры (ICQ, WhatsApp, Viber);

3) базы данных (Google, Wolfram Alpha, Bing, Wikipedia, Yelp) и базы данных, опубликованные в результате атак на различные сервисы;

4) другие источники, которые являются открытыми для создателей «Глаза Бога» на основании заключенных договоров:

– «Контур.Фокус» – сервис для проверки российских и зарубежных контрагентов (позволяет получить много полезной информации: залоги, выписки из ЕГРЮЛ и ЕГРИП, банкротство, отчеты об объектах недвижимости и многое другое);

– «СПАРК» также является сервисом проверки контрагентов (имеет такие данные, как сведения о платежной дисциплине компаний, материалы СМИ, информация о зарубежных юридических лицах; предоставляет доступ к данным кредитного бюро, нотариата, Росреестра);

– Solaris – сетевая информационная среда глобальных компаний.

Для осуществления поиска необходимо оплатить подписку в «Телеграме».

Сервис «Глаз Бога» на данный момент является одним из наиболее эффективных сервисов, поскольку располагает огромными базами данных, в том числе опубликованных в результате взлома сервисов, обладающих достоверной информацией о пользователях, в частности их персональными данными.

2.5. Программное обеспечение для поиска сведений о физических и юридических лицах в сети Интернет по фотографии

Наряду с программным обеспечением для поиска информации о физических и юридических лицах в сети Интернет, реализующим комплексный подход по набору поисковых реквизитов,

известны программные продукты с меньшими функциональными возможностями для поиска сведений по фотографии. Такое программное обеспечение может представлять интерес для сотрудника ОВД при решении задачи поиска различных сведений о физическом лице по его фотографии.

Система распознавания лиц FindClone

Findclone – программное обеспечение, осуществляющее поиск лиц по фотографии [17], основанное на сложных операциях – от обычного распознавания лиц до биометрических измерений. Принцип работы алгоритма, заложенного в технологии, состоит в самообучении нейросети после выполнения каждого нового поиска. Путем многократных проб она самостоятельно находит необходимые параметры и взаимосвязи, интерпретирует полученную информацию в модель для последующего сравнения с другими моделями.

Недостатком данного сервиса является невозможность поиска при наличии следующих условий:

– представленная для поиска фотография выполнена со значительно низким качеством;

– фотография имеет низкое разрешение и (или) маленький размер;

– черты лица плохо просматриваются;

– фотография сделана со спины, сбоку, представляет собой лишь силуэт человека;

– в отдельных случаях возникают трудности в определении лиц на групповых фотографиях.

Использование данного инструмента осложнено процедурой регистрации, которая производится путем принятия вызова на личный номер телефона. После ввода пароля в форму, соответствующего последним пяти цифрам входящего звонка, будет осуществлен переход в личный кабинет. После загрузки фотографии отображаются предположительные профили аккаунтов социальной сети «ВКонтакте» или Instagram, которым она может принадлежать. Доступны активные ссылки, по которым можно осуществить переход.

Главным достоинством FindClone является отображение недоступных для публичного просмотра фотографий из закрытых настройками приватности профилей социальной сети. Сервис предоставляет услуги на порядок качественнее иных аналогичных программных решений и является одним из немногих в мире, осуществляющих функции подобного рода быстро и точно.

Сервис поиска людей по фотографии search4faces

Сервис позволяет осуществлять поиск по лицам, имеющим персональные страницы в социальных сетях «Одноклассники» и «ВКонтакте» [18]. Сервис предоставляет услуги на безвозмездной основе на русском языке и результат работы за короткий промежуток времени.

При осуществлении загрузки фотографии алгоритм автоматически выделяет область лица и предоставляет первые результаты возможных совпадений. Важно отметить, что система обладает рядом недостатков: точность соответствия в отдельных случаях невысока, результаты поиска могут быть лишь похожи на оригинал, но не соответствовать ему (рис. 12).

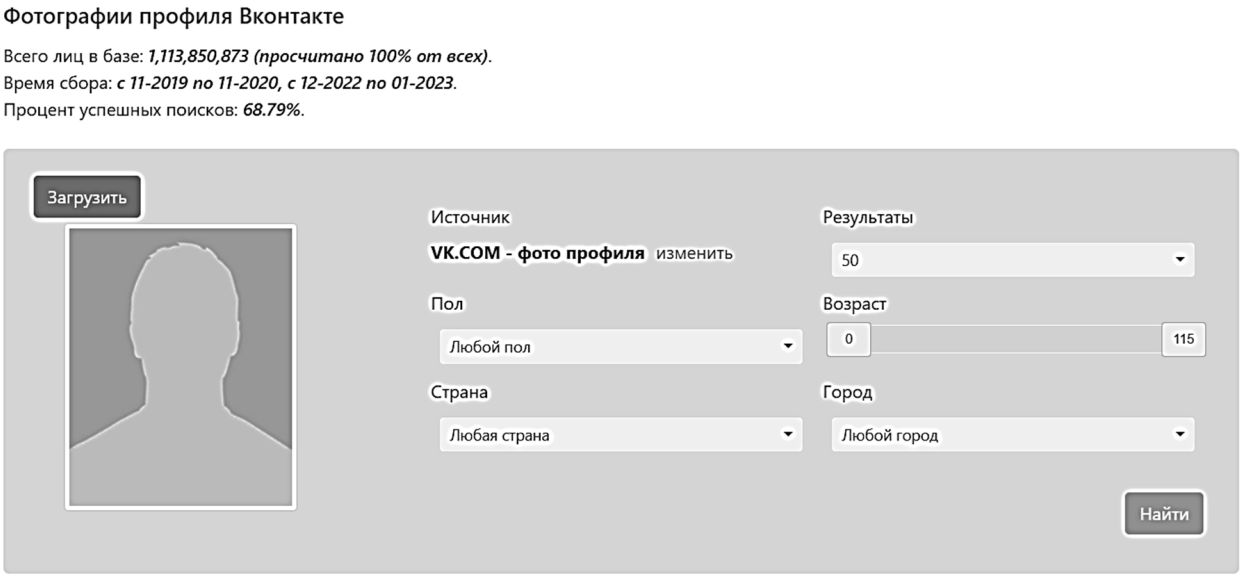


Рис. 12. Интерфейс сервиса поиска людей по фотографии search4faces

К достоинствам данной технологии можно отнести наличие параметров и настроек поиска:

– по половой принадлежности;

– по возрасту;
– по стране проживания и городу;
– по источнику поиска.

Каждая найденная фотография представляет собой ссылку на ту или иную социальную сеть. Точность отображаемых результатов представлена процентами в зависимости от соответствия оригиналу.

Если диапазон совпадения составляет 53–60%, то степень достоверности высокая, однако существует необходимость в повторном поиске посредством других сервисов. При коэффициенте более 60% результат считается более точным, но также требует визуальной проверки.

Главным недостатком данной технологии является сопоставление загруженной фотографии с фотографиями, установленными на главной странице профиля «ВКонтакте» и «Одноклассники», в то же время с иными веб-сайтами и социальными сетями работа не осуществляется, что значительно снижает вероятность определения. Также технология неэффективно работает с затемненными фотографиями и сделанными в пол-оборота.

OSINT-браузер Venator

На тематических сайтах сети Интернет встречаются программные надстройки на известные браузеры, позволяющие собирать различные сведения. Рассмотрим их работу на примере OSINT-браузера Venator – инструмента, который предназначен для сбора и анализа информации в Интернете на основе открытых источников. Проект Venator создан для развития, популяризации и улучшения направления OSINT на территории СНГ. Проект представляет собой расширение, поддерживаемое браузерами Chrome и Firefox, имеющее дополнительные надстройки, позволяющие осуществлять эффективный поиск информации по открытым источникам.

Venator состоит из нескольких модулей, которые позволяют проводить различные виды поиска:

– геолокация (позволяет осуществлять поиск информации на основе местоположения);

− хэштег (позволяет искать информацию на основе хэштегов в социальных сетях);

− личность (позволяет искать информацию на основе имени и фамилии);

− компания (позволяет искать информацию на основе имени компании).

Venator также поддерживает плагины, которые позволяют расширить функциональность инструмента:

− валидатор электронной почты (проверяет, является ли адрес электронной почты действительным);

− анализатор изображений (позволяет проводить анализ изображений, включая определение местоположения снимка, даты съемки и даже лиц на фото);

− определитель технологий (позволяет определить, какие технологии используются на конкретном веб-сайте);

− анализатор PDF (позволяет анализировать содержимое PDF-файлов, включая текст и метаданные);

− определитель социальных сетей (позволяет определить, какие социальные сети используются конкретным сайтом).

Venator имеет множество функций, которые позволяют производить поиск, анализировать, фильтровать и визуализировать данные из различных источников. Некоторые из основных функций Venator включают в себя:

– модули поиска позволяют искать данные в социальных сетях, новостных и блоговых источниках, на картах, в документах, изображениях;

– глубокий анализ данных позволяет анализировать и фильтровать данные по различным параметрам, таким как дата, язык, географическое положение, можно также использовать регулярные выражения для более точного поиска;

– извлечение метаданных позволяет извлекать метаданные из изображений, документов и других файлов, таких как GPS-координаты, даты, временные метки;

– визуализация данных позволяет представлять данные в виде таблиц, графиков, карт и других форматов;

– работа с плагинами предполагает выполнение дополнительных задач, таких как сканирование портов, анализ сетевого трафика;

– совместимость с различными операционными системами: Windows, MacOS и Linux, а также в качестве расширения для браузеров Chrome и Firefox;

– работа с данными и поиск на различных языках.

Это лишь некоторые из функций Venator, которые могут быть полезными для сотрудников ОВД.

2.6. Проведение поиска с использованием символов и операторов в системах «Яндекс» и «ВКонтакте»

Описываемые здесь возможности поиска с использованием символов и операторов в системах «Яндекс» и «ВКонтакте» показывают примеры осуществления запросов на указанных ресурсах, популярных в России и за ее пределами. По аналогии подобные решения можно применять на других известных ресурсах.

Наиболее привычным методом поиска информации с точки зрения интуитивного поведения пользователя в сети Интернет является обращение к стандартным поисковым системам. На данный момент времени поисковые системы также обладают достаточно обширным функционалом для осуществления поиска информации на веб-ресурсах, например индексированным и полнотекстовым поиском и поиском по картинке.

Важно отметить, что первоначально целью данных систем не являлось непосредственное хранение массивов данных, однако в процессе их функционирования способ просмотра и сбора информации на многочисленных сайтах и последующее ее копирование в собственные базы данных был определен как наиболее быстрый и эффективный способ поиска информации.

Важно отметить, что фундаментальными критериями качества работы поисковой системы выступают релевантность – степень соответствия определенного запроса и результата на этот запрос, полнота базы данных интернет-ресурсов, а также принятие во внимание морфологии языка.

Информация стандартизировано представляется и хранится в форме, которая приемлема для автоматизированной обработки. При осуществлении поиска средствами поисковой системы «Яндекс» происходит процесс обращения к базам данных соответствующих поисковых машин, где запрос анализируется и сопоставляется, в результате чего система определяет наиболее релевантные результаты и предоставляет ссылки на соответствующие источники.

Алгоритм обработки пользовательских запросов непрерывно совершенствуется, однако для более результативного нахождения необходимой информации важно использовать универсальные вспомогательные команды в виде операторов поисковых запросов.

Например, заключение запроса в кавычки необходимо при поиске такой информации, как фамилия или имя определенного лица в сети Интернет, а также фразы по однозначному и точному соответствию. Следует отметить, что результатом поиска с таким оператором будет строгая установленная запросом последовательность слов, содержащаяся в тексте. Учитывая данный факт, рекомендуется применять различные сочетания слов и их порядок, в противном же случае поиск будет безуспешен. Например: «Петров Петр Петрович», или «Петр Петрович Петров», или «Петров П.П.» [22].

Поисковые системы, как правило, успешно справляются с возложенной на них задачей и результат запроса обычно представляет собой большое количество не всегда нужной информации. Лишние сведения исключаются из выдачи путем указания знака тире перед ними. Так, чтобы исключить из результатов запроса всех художников, в нашем случае нужно ввести в поисковую строку следующее: «Петров Петр Петрович» – художник.

Если известно, что определенный веб-сайт или другой интернет-ресурс содержит необходимые сведения, следует обозначить его в поисковом запросе. Например: *site:*novosti.ru «Петров П.П.».

Если на веб-сайте или любом другом ресурсе существуют документы различного расширения, в которых указана фамилия, имя лица, необходимо ввести следующее выражение: site:novosti.ru filetype:txt Петров. Результатом такого запроса бу-

дут являться ссылки на материалы, содержащие определяющее слово, в указанном случае «Петров».

Важной особенностью процесса производства поиска посредством описанных операторов является невозможность его осуществления по социальным сетям ввиду их сложного устройства. Большинство информации, находящейся в их базах данных, недоступно для индексирования алгоритмом поисковых сервисов. Вследствие этого для получения объективной картины необходимо осуществлять поиск лиц отдельно и непосредственно в каждой социальной сети. В остальных же случаях, если имя или данные о лице когда-либо попадали на просторы сети Интернет, то информация об этом в обязательном порядке попадет в отображаемые по запросу результаты.

Рассмотрим специфику поиска информации об интересующем лице непосредственно в социальных сетях на примере сети «ВКонтакте» [23]. Для выполнения данных действий следует пройти регистрацию. В целях безопасности необходимо создать вымышленный аккаунт в интересующей социальной сети, так как авторизация предполагает расширенный спектр возможностей.

Механизм осуществления поиска может быть выполнен по следующим параметрам.

Поиск по комментариям или вторичным публикациям записей:

– type:copy;

– type:reply.

Аналогично рассмотренному раннее примеру можно исключить из результатов лишнюю информацию путем постановки тире перед словом:

– -type:reply

Ниже представлена группа операторов, устанавливающих параметры на вложения в запись, комментарий или перепубликацию. С их помощью можно искать фотографии, видеофайлы, аудиофайлы, граффити, заметки, опросы, ссылки, документы, альбомы, содержащие только текст записи.

Операторы поиска во вложении:

– has:photo (фотографии);

– has:video (видео);

– has:audio (аудиофайла);

– has:note (заметки);
– has:poll (опроса);
– has:link (ссылки);
– has:doc (документа);
– has:album (альбома);
– has:none (публикации без вложений).

Следующая группа операторов используется для поиска записи с установленным количеством лайков (10, 100, 1000):

– likes:10;
– likes:<100;
– likes:>1000.

Для поиска публикаций, которые могут содержать ссылки на сайты или домены, применяются следующие операторы:

– url:сайт;
– domain:домен.

Операторы поиска копии определенной фотографии: copy:photo6454564651.

Для отображения настоящего id пользователя существует сервис vk.com/linkapp. Описанные операторы следует применять в различных сочетаниях, так результаты запросов будут иметь более конкретный характер. Социальная сеть «Одноклассники» более консервативна и не имеет подобных операторов. Пользователю данной социальной сети первоначально предоставлен расширенный поиск, предполагающий такие параметры, как город, место рождения, образовательное учреждение, дата рождения и др.

Благодаря использованию специальных символов и сочетаний клавиш сотрудники органов внутренних дел могут самостоятельно, без привлечения специалистов, обладающих знаниями в сфере информационных технологий, осуществлять эффективный поиск информации в сети Интернет, в том числе самостоятельно проводить анализ полученных данных и выборку полезных данных на фоне избыточности информации в сети Интернет.

2.7. Альтернативные узконаправленные сервисы поиска информации в сети Интернет

Среди рассматриваемых ранее сервисов поиска сведений в сети Интернет существуют сервисы, которые выполняют более точечные задачи в общем процессе поиска информации о физических и юридических лицах. Использование подобных инструментов может дать больше сведений в сравнении с комплексным программным обеспечением в определенных обстоятельствах. Для получения объективных результатов рекомендуется их использование в комбинации с вышерассмотренными программами.

Перечень программного обеспечения (табл. 4) был получен по запросу Краснодарского университета МВД России о составлении перечня программного обеспечения, используемого для OSINT, от научно-технического центра «Вулкан» [24]. Научно-технический центр «Вулкан», основываясь на практическом опыте реализации проектов создания комплексных систем обеспечения информационной безопасности, а также проектов по анализу защищенности, предлагает проведение анализа данных в открытых источниках (OSINT) и оценки уровня осведомленности персонала в вопросах информационной безопасности методами социальной инженерии. Перечень состоит из программного обеспечения, которое может использоваться в поиске информации, интересующей сотрудника ОВД.

Таблица 4

Перечень программного обеспечения OSINT

Ресурсы для проверки пользовательского имени		
Наименование	Назначение	Ссылка
Namechk	Сервис позволяет проверять пользовательское имя (username) в социальных сетях и сервисах, а также доменные имена. Способен проверять до 100 ресурсов	https://namechk.com

Продолжение табл. 4

Ресурсы для проверки пользовательского имени		
Наименование	Назначение	Ссылка
Checkusernames	Сервис позволяет проверять пользовательское имя (username) в социальных сетях и сервисах, а также доменные имена. Способен проверять до 160 ресурсов	https://checkusernames.com
Ресурсы с базами данных о людях		
Наименование	Назначение	Ссылка
ThatsThem people search	Сервис содержит персональные данные людей и позволяет осуществлять поиск по одному из типов данных	https://thatsthem.com
Melissa Personator	Сервис содержит персональные данные людей и позволяет осуществлять поиск по одному из типов данных. Количество запросов ограничено, необходима регистрация через почту, почту следует подтверждать	https://www.melissa.com/v2/lookups/personator
TruePeopleSearch	Сервис позволяет осуществлять поиск по базам персональных данных людей	https://truepeoplesearch.net
BeenVerified	Это веб-сервис, в котором собрана информация о людях, в основном проживающих в США. Сервис не является бесплатным	https://beenverified.com
Xlek.com	Сервис позволяет осуществлять поиск по базам персональных данных людей	https://xlek.com
Nuwber		https://nuwber.com
Radaris		https://radaris.com
Social Searcher	Сервис осуществляет поиск аккаунтов или упоминаний в популярных социальных сетях	https://www.social-searcher.com

Продолжение табл. 4

Веб-ресурсы для поиска изображений		
Наименование	Назначение	Ссылка
Google Images	Поисковая система позволяет находить изображение по переданному запросу или осуществлять обратный поиск по изображению и показывать ресурсы, где изображение используется	https://images.google.ru
Yahoo! Images		https://ru.images.search.yahoo.com
Bing Images		https://www.bing.com/images
Яндекс.Картинки		https://yandex.ru/images
TinEye	Сервис позволяет осуществлять обратный поиск по изображению и показывать ресурсы, где изображение используется	https://tineye.com
RevEye Reverse Image Search	Расширение Google для поиска по изображению на сервисах Google, Bing, Yandex, TinEye and Baidu	https://chrome.google.com/webstore/detail/reveye-reverse-image-sear/keaaclcjhehbbapnphnmpiklalfhelgf
Picsearch	Сервис для поиска изображений по текстовому запросу, позволяет проиндексировать их значительное количество	https://www.picsearch.com
Сервисы и инструменты для проверки данных в базах с утечками данных		
Наименование	Назначение	Ссылка
Pwndb	.onion-ресурс позволяет получить «незацензуренные» данные из собрания, содержащего 1,4 млрд записей, не требуя финансовых вложений и регистрации на ресурсе	Darknet
Haveibeenpwned	Веб-сервис предназначен для поиска по базам данным, содержащим «утекшие» данные. Услуги поиска предоставляются бесплатно и не требуют регистрации, но ресурс не предоставляет сами данные	https://haveibeenpwned.com

Продолжение табл. 4

Сервисы и инструменты для проверки данных в базах с утечками данных		
Наименование	Назначение	Ссылка
DeHashed	Веб-сервис предоставляет возможность проверки присутствия передаваемых данных в базах данных с утечками, сообщая, в каких именно коллекциях участвует адрес, может предоставить непосредственно «слитые» данные при оформлении платной подписки	https://dehashed.com
H8mail	Это кроссплатформенный инструмент, предназначенный для агрегации поиска учетных данных и некоторых других типов данных на нескольких сервисах и среди известных коллекций с утечками данных	https://github.com/khast3x/h8mail
Валидаторы почтовых адресов		
Наименование	Назначение	Ссылка
Simple Email Reputation	Сервис для проверки существования электронного адреса	https://emailrep.io
Mailboxvalidator	Сервис позволяет оценить валидность электронного адреса	https://www.mailboxvalidator.com
Melissa Global Email Check	Веб-сервис позволяет проверить валидность электронного адреса и оценить возможность доставки писем на данный адрес	https://www.melissa.com/v2/lookups/emailcheck/email
Email Permutator	Сервис перебирает входные данные и популярные паттерны и выдает список возможных адресов, но без валидации	http://emailpermutator.com/permutator
Сервисы и инструменты для извлечения метаданных изображений		
Наименование	Назначение	Ссылка
Jeffrey's Image Metadata Viewer	Сервис извлекает метаданные из изображения, которое может передаваться как в виде URL-адреса, так и в виде файла	http://exif.regex.info/exif.cgi
metapicz		http://metapicz.com/#landing

Продолжение табл. 4

Сервисы и инструменты для извлечения метаданных изображений		
Наименование	Назначение	Ссылка
Get-metadata	Веб-сервис позволяет извлекать метаданные изображений, а также метаданные документов и видео	https://www.metadata2go.com
JPEGsnoop	Бесплатное приложение для Windows, которое извлекает и анализирует метаданные файлов JPEG, MotionJPEG, AVI и Photoshop	https://github.com/ImpulseAdventure/JPEGsnoop
ExifTool	Инструмент для чтения, записи и редактирования метаданных самых различных файлов	https://github.com/exiftool/exiftool
Сервисы для поиска информации по номеру телефона		
Наименование	Назначение	Ссылка
ReversePhoneLookup	Сервис позволяет осуществлять поиск информации по номеру телефона	https://free-lookup.net
Whocalled		https://who--called.com
International Numbering Plans	Веб-сервис позволяет осуществлять поиск информации по международным телефонным номерам, при этом гарантированно определяет страну, регион и провайдера сети	https://www.numberingplans.com/?page=home
SpyDialer	SpyDialer позволят осуществлять поиск по номеру телефона, относящемуся к США	https://www.spydialer.com
Free Carrier Lookup	Сервис позволяет определить провайдера телефонной связи	https://freecarrierlookup.com
Phone Lookup	Сервис предоставляет информацию о телефонных номерах США	https://www.phonelookup.com
FoneFinder	Сервис предоставляет информацию о телефонных номерах США и Канады, но может осуществлять поиск и по номерам других стран	http://www.fonefinder.net

Продолжение табл. 4

Сервисы для поиска информации по номеру телефона		
Наименование	Назначение	Ссылка
Hlrlookup	Сервис позволяет через проверку подключений к базам данных HLR определить принадлежность данного номера определенному оператору и стране, нужна регистрация	https://www.hlrlookup.com
Numberway	Сервис позволяет выбрать страну и выдает в результате список ресурсов, где может быть найдена информация о телефоне, относящемся к данной стране	https://www.thisnumber.com
IoT и IP cams		
Наименование	Назначение	Ссылка
Shodan	Shodan – это поисковая система, специализирующая на поиске определенных устройств и типов устройств, подключенных к сети Интернет	https://www.shodan.io
Сервисы для анализа аккаунтов Twitter		
Наименование	Назначение	Ссылка
foller.me	Веб-сервис для анализа профиля в Twitter	https://foller.me
Follerwonk	Веб-сервис для анализа профиля в Twitter, сравнения подписок и подписчиков двух или трех пользователей, поиска профиля	https://followerwonk.com
Mentionmapp	Веб-сервис позволяет анализировать социальные связи и популярные темы по упоминаниям и хэштегам в Twitter	https://mentionmapp.com

Продолжение табл. 4

Ресурсы для поиска файлов на ftp-серверах		
Наименование	Назначение	Ссылка
Mmnt.ru	Проект «Мамонт» – поисковая система для обычного поиска в сети Интернет и для поиска файлов на публичных ftp-серверах	https://www.mmnt.ru
Metabot.ru	metabot.ru – поисковая система, позволяющая производить поиск ресурсов в российском сегменте сети Интернет, глобальный поиск и поиск файлов	https://www.metabot.ru
Adapt Prospector	Расширение для Google Chrome, позволяющее извлекать контактные данные из профиля в социальной сети LinkedIn, результатов поиска профилей LinkedIn или любого веб-ресурса	https://prospector.adapt.io
Фреймворки		
Наименование	Назначение	Ссылка
DataSploit	DataSploit позволяет получить информацию о конкретном пользователе, сайте или наборе различных входных данных	https://github.com/DataSploit/datasploit
Intrigue Core	Фреймворк для автоматизации OSINT	https://core.intrigue.io
Maltego CE	Инструмент для визуализации данных и автоматизированного поиска	https://www.maltego.com
OSRFramework	Фреймворк осуществляет базовые действия, входящие в методику OSINT	https://github.com/i3visio/osrframework
Recon-ng	Фреймворк для автоматизации разведки на основе открытых источников	https://github.com/lanmaster53/recon-ng
SpiderFoot	Инструмент для OSINT, автоматически собирающий информацию из более чем сотни источников	https://www.spiderfoot.net
Lampyre	OSINT фреймворк	https://lampyre.io

Продолжение табл. 4

Другие устанавливаемые инструменты		
Наименование	Назначение	Ссылка
Email2phonenumber	Предназначение скрипта состоит в автоматизации процесса поиска телефонного номера при известном адресе электронной почты	https://github.com/martinvigo/email2phonenumber
FOCA	Инструмент, позволяющий осуществлять поиск метаданных и скрытой информации в сканируемых документах	https://github.com/ElevenPaths/FOCA
«Instagram» OSINT Tool	Это кроссплатформенный инструмент, предназначенный для извлечения информации из профиля в социальной сети Instagram	https://github.com/sc1341/InstagramOSINT
PhoneInfoga	Инструмент предназначен для поиска информации по номеру телефона из доступных источников	https://github.com/sundowndev/phoneinfoga
Sherlock	Это кроссплатформенный инструмент, позволяющий осуществлять поиск профилей в различных социальных сетях и сервисах по имени пользователя (username)	https://github.com/sherlock-project/sherlock
SimplyEmail	Инструмент позволяет на основе доменного имени компании осуществлять поиск электронных адресов с данным доменом	https://github.com/SimplySecurity/SimplyEmail
TheHarvester	Инструмент для поиска почтовых адресов по доменному имени компании в различных публичных поисковых системах и сервисах	https://github.com/laramies/theHarvester
Infoga		https://github.com/m4ll0k/Infoga
Twint	Инструмент позволяет извлекать и анализировать твиты пользователя социальной сети Twitter	https://github.com/twintproject/twint
Zen	Инструмент, предназначенный для поиска электронных адресов пользователей платформы Github	https://github.com/s0md3v/Zen

Окончание табл. 4

Основные поисковые системы		
Наименование	Назначение	Ссылка
Google	Лидирующая поисковая система	https://www.google.ru
Bing	Поисковая система, одна из «поисковых гигантов»	https://www.bing.com
Yandex		https://yandex.ru
WikiLeaks	Поисковая система для поиска в подвергнутых цензуре и сокрытых документах	https://wikileaks.org
Инструменты для анализа профиля Instagram		
Наименование	Назначение	Ссылка
Search My Bio	Инструмент, предназначенный для поиска слов в Bio пользователей	https://www.searchmy.bio
SaveIG	Ресурс позволяет анонимно скачивать фотографии, видео и истории	https://imginn.com
Spatulah	Ресурс позволяет сохранить комментарии к публикации для дальнейшего анализа	https://spatulah.com
Nuga.app	Сервисы для поиска аккаунта Instagram по номеру телефона	https://nuga.app

Полученный перечень программного обеспечения, реализующий функцию поиска конкретных сведений, необходимых для проведения расследований по административным и уголовным делам, позволит сотрудникам органов внутренних дел самостоятельно проводить поиск, сбор, обобщение и поверхностный анализ необходимой информации.

Контрольные вопросы

1. Какое программное обеспечение называется поисковым?
2. Какие виды поисковых систем вы знаете? Приведите примеры.
3. Из чего состоит поисковое программное обеспечение?

4. Для чего предназначено и какая технология используется в программном обеспечении FindFace?

5. Какие задачи позволяет решать поисковая система «СЕУС», из чего состоит и какими возможностями она обладает?

6. Для чего предназначено программное обеспечение VK.Watch и в чем заключается алгоритм его применения?

7. Что представляет собой программное обеспечение «Глаз Бога», для чего предназначено и какие у него возможности?

8. Какие возможности у системы мониторинга «Демон Лапласа», какие модули она поддерживает?

9. Какие возможности имеет система распознавания лиц FindClone и сервис search4faces?

10. Для каких задач может использоваться сервис Web archive?

11. Какие возможности обеспечивают инструменты OSINT-браузера Venator?

12. Для чего предназначена система «Медиалогия», из чего состоит и какие параметры она использует?

13. Что представляет собой программно-аппаратный комплекс «Крибрум», из каких систем он состоит?

14. Какие возможности поисковой системы «Яндекс» дает применение символов и операторов?

15. Какие возможности по поиску информации дает использование символов и операторов в социальной сети «ВКонтакте»?

16. Какие вы знаете альтернативные инструменты поиска информации в сети Интернет по узким направлениям?

Глава 3. Выбор специализированного программного обеспечения для осуществления поиска информации для органов внутренних дел в сети Интернет

3.1. Классификация исходных данных для поиска сведений в сети Интернет

При осуществлении поиска информации в открытых источниках сети Интернет о физических и юридических лицах необходим особый подход к каждой конкретно взятой ситуации. Основополагающими условиями выбора специализированного программного обеспечения являются исходные данные о лице, в отношении которого проводятся оперативно-поисковые мероприятия.

В целях адаптации массива имеющихся исходных данных к возможностям рассмотренного поискового программного обеспечения была разработана классификация (рис. 12), основной задачей которой является соотнесение поисковых контрольных точек с массивом исходных данных (классами поиска).

Так, исходя из полученной классификации, можно выделить следующее.

1. Класс поиска «Биография» можно разбить на методы поиска по точкам:

– место рождения физического лица;

– школа, в которой обучался человек;

– университет, в котором обучался человек;

– место работы;

– информация о службе в армии.

2. Класс поиска «Документы» можно разбить на методы поиска по точкам:

– паспортные данные физического лица;

– водительские права;

– страховое свидетельство;

– ИНН;

– документы, подтверждающие окончание образовательного учреждения.

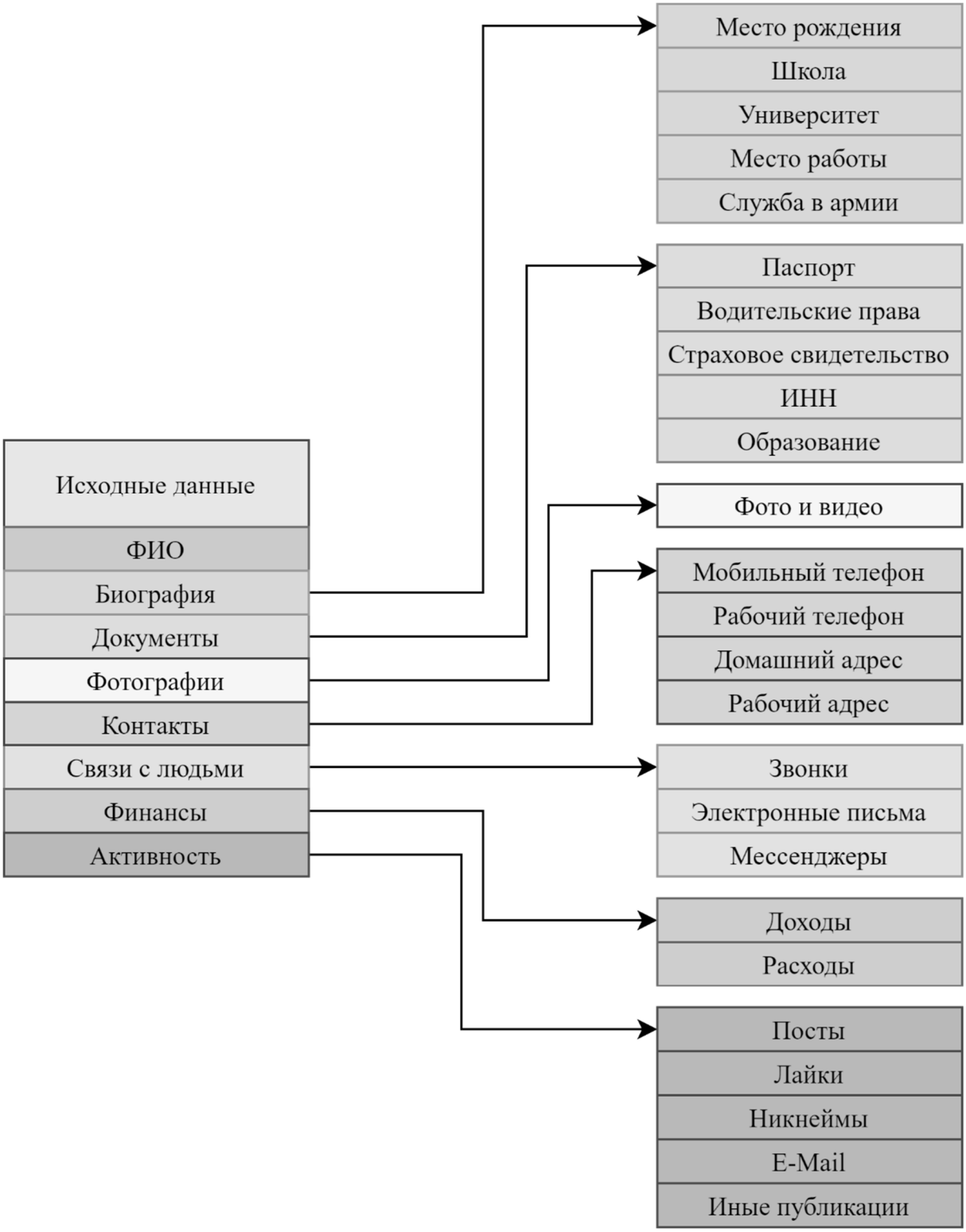


Рис. 12. Классификация исходных данных

3. Класс поиска «Контакты» можно разбить на методы поиска по точкам:

– мобильный телефон;
– рабочий телефон;
– домашний адрес;

– рабочий адрес.

4. Класс поиска «Связи с людьми» можно разбить на методы поиска по точкам:

– история звонков физического или юридического лица;

– переписка в электронной почте;

– переписка в мессенджерах.

5. Класс поиска «Финансы» можно разбить на методы поиска по точкам:

– доходы физического или юридического лица;

– расходы физического или юридического лица.

6. Класс поиска «Активность» можно разбить на методы поиска по точкам:

– посты физического лица в социальных сетях;

– лайки физического лица в социальных сетях;

– используемые никнеймы в различных сервисах сети Интернет;

– используемые адреса электронной почты;

– иные публикации.

Как уже было отмечено, классификация приведена на основе функциональных возможностей программного обеспечения, рассмотренного в предыдущем разделе учебного пособия для того, чтобы сотрудник ОВД мог эффективно соотнести исходные данные с данными, формируемыми программным обеспечением.

3.2. Выбор программного обеспечения для поиска сведений в сети Интернет

На основе приведенного в первом разделе перечня российского программного обеспечения для поиска сведений о физических и юридических лицах в открытых источниках сети Интернет далее приведено краткое описание с рекомендациями по использованию в деятельности ОВД.

1. FindFace. Подходит для поиска информации о человеке по фотоизображению, позволяет получить информацию о человеке по его странице в социальной сети. Рекомендуется к исполь-

зованию при наличии у сотрудника ОВД фотоизображения интересующего лица.

2. FindClone. Является аналогом FindFace и позволяет найти информацию о человеке по его фотоизображению, результатом поиска является страница в социальной сети. Рекомендуется к использованию при наличии у сотрудника ОВД фотоизображения интересующего лица. Является наиболее эффективным инструментом поиска в категории подобных инструментов.

3. VK.watch. Позволяет находить посты, лайки, комментарии, удаленные фото и видео пользователя социальной сети «ВКонтакте». Рекомендуется использовать в случае, если известна ссылка профиля лица, в отношении которого производятся поисковые мероприятия. Недостатком сервиса является его монетизация, поэтому, по экономическим соображениям, следует использовать его в последнюю очередь и в случае, если иные сервисы не дали результатов.

4. Поисковые системы являются эффективным дополнением к иным поисковым инструментам. Наиболее эффективны в случае наличия в перечне исходных данных строковых выражений, которые могут идентифицировать физическое или юридическое лицо.

5. «СЕУС». Поисковое программное обеспечение «СЕУС» позволяет наиболее эффективно анализировать посты и лайки в социальной сети «ВКонтакте». Разработчики программного обеспечения активно сотрудничают с правоохранительными органами и по соответствующему запросу могут предоставить аутентификационные данные для проведения тестовых запросов к базам данных «СЕУС». Рекомендуется использовать данное программное обеспечение для поиска информации о физических лицах в социальной сети «ВКонтакте».

6. «Глаз Бога». Представляет собой достаточно универсальную платформу для поиска информации о физических и юридических лицах, позволяет производить поиск по различным типам исходных данных, во второй главе учебного пособия представлено расширенное описание работы данного программного обеспечения.

7. Search4faces. Представляет собой аналог FindFace и FindClone, может быть использован для поиска информации

о лице по его фотоизображению. Производит поиск информации в базах данных, сформированных на основе анализа социальных сетей «ВКонтакте» и «Одноклассники».

8. «Демон Лапласа». Комплексное программное обеспечение, включающее в себя несколько модулей. Позволяет производить анализ ситуации в сети Интернет на текущий момент времени, прогнозировать события. Функционал программного обеспечения предполагает его использование в качестве превентивной меры в целях предупреждения преступлений и правонарушений, а не для расследования отдельных, уже случившихся инцидентов.

9. Web archive. Сервис, который хранит в своих базах информацию о состоянии веб-ресурсов в определенные промежутки времени, делает слепки визуальной составляющей веб-страницы. Рекомендован к использованию в случае наличия в массиве исходных данных страницы социальной сети лица, в отношении которого производится сбор материала. Использование Web archive обусловлено тем, что с недавних пор в функционал социальных сетей введена возможность скрытия своего профиля, примером может послужить социальная сеть «ВКонтакте». Web archive позволит анонимно просмотреть информацию о состоянии страницы до момента ее сокрытия владельцем.

10. Операторы социальной сети «ВКонтакте». Данный способ поиска информации на сегодняшний день является недостаточно эффективным в силу установленной социальной сетью политики конфиденциальности и возможности сокрытия профиля пользователем. Однако операторы позволяют производить поиск по хэштегам, комментариям и иным записям, которые находятся в открытом доступе.

11. Программно-аппаратный комплекс «Крибрум» – развитый комплекс сбора, мониторинга и анализа данных социальных медиа в режиме реального времени, включает в себя платформу сбора и хранения данных и системы разнообразного анализа больших данных и поведения пользователей социального пространства.

12. Альтернативные сервисы поиска информации могут быть полезны практически в любой ситуации, данные сервисы позволяют выполнять практически полный комплекс поисковых мер, однако главным недостатком является их децентрализация и

отсутствие возможности автоматической генерации классифицированной и обобщенной информации о лице, интересующем сотрудника ОВД.

Для наиболее эффективного применения сотрудниками ОВД специализированного программного обеспечения для поиска информации о физических и юридических лицах в открытых источниках сети Интернет предлагается схема с указанием программного обеспечения для поиска информации, исходя из перечня исходных данных (рис. 13).

Предлагается достаточное количество программного обеспечения, начиная от узконаправленных онлайн-сервисов и заканчивая сложными программными комплексами с продвинутыми алгоритмами, где предусмотрена одновременная работа нескольких сложных модулей, каждый из которых выполняет свою функцию по мониторингу, анализу, формированию статистики и поиску интересующих сведений.

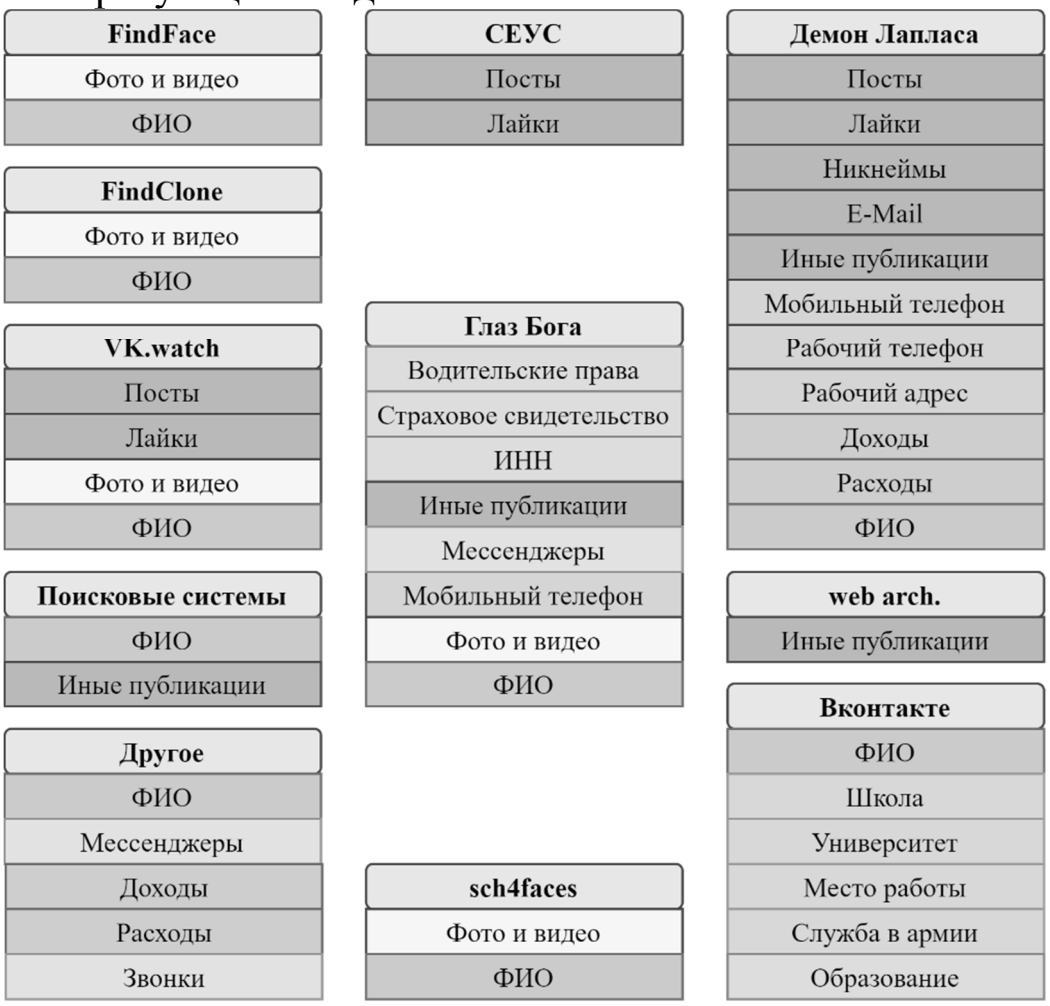


Рис. 13. Рекомендации по использованию поискового программного обеспечения

Контрольные вопросы

1. Каким образом нужно осуществлять выбор программного обеспечения для поиска информации в открытых источниках сети Интернет?
2. Какие исходные данные для поиска информации в сети Интернет вы можете перечислить?
3. Какое программное обеспечение для поиска информации в сети Интернет вы можете рекомендовать коллеге, в каких ситуациях и почему?

Заключение

Как показывает практика, на сегодняшний день можно в достаточно короткие сроки без серьезных финансовых вложений получить интересующую информацию о физическом или юридическом лице без использования дорогостоящих программных средств. Стоит отметить, что, в зависимости от ситуации, не во всех случаях стоит прибегать к использованию сложных программных модулей: в сети Интернет существует множество инструментов, предоставляющих сведения о лицах безвозмездно, в первую очередь рекомендуется использовать именно эти сервисы. В руках компетентного сотрудника использование специализированного программного обеспечения может дать достаточное количество информации о интересующем лице. Исходя из проведенного обзора программного обеспечения, сотруднику ОВД для использования рекомендуются следующие программные платформы.

1. Программно-аппаратный комплекс «Крибрум» – развитый комплекс сбора, мониторинга и анализа данных социальных медиа в режиме реального времени.

2. Поисковая система ««СЕУС»» – для поиска информации в открытых источниках сети Интернет о физических и юридических лицах.

3. Автоматизированная система круглосуточного мониторинга и сбора данных «Демон Лапласа» – для предварительного анализа данных и предупреждения преступлений и правонарушений.

Следует также отметить перечень альтернативного узконаправленного программного обеспечения для поиска информации в сети Интернет; в некоторых ситуациях его использование может дать высокие результаты с минимальными затратами.

Литература

1. Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации: приказ МВД России от 29.12.2022 № 1110. Доступ из справ.-правовой системы «Гарант».

2. Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2022 года. URL: https://мвд.рф/reports/item/35396677 (дата обращения: 13.02.2023).

3. Ведущая платформа для автоматизации аналитических подразделений. URL: http://www.anbr.ru (дата обращения: 13.02.2023).

4. Галактионова Ю.Ю. Поисковая система «СЕУС» как инструмент исследования протестных настроений // Современное общество: вопросы теории, методологии, методы социальных исследований. 2019. Т. 1. С. 67–71

5. Кокурин Г.А. Правовая регламентация оперативно-технических мероприятий // Российский юридический журнал. 2015. № 5. С. 108–111.

6. Кондратьев А. На основе открытых источников. Архивная копия от 22 сентября 2013 г. на Wayback Machine // ВПК. 2009. № 36(302).

7. Масалович А. Конкурентная разведка. URL: https://am.news (дата обращения: 13.02.2023).

8. Молоков В.В. Эффективные способы получения открытой информации в сети Интернет // Novaum.ru. 2017. № 9.

9. Найди профили человека в соцсетях по его фотографии. URL: https://search4faces.com (дата обращения: 13.02.2023).

10. Осипенко А.Л., Луговик В.Ф. Проблемы доступа правоохранительных органов к скрываемой компьютерной информации при раскрытии преступлений // Общество и Право. 2021. № 2(76).

11. Официальный сайт ООО «СЕУСЛАБ». URL: https://www.seuslab.ru (дата обращения: 13.02.2023).

12. Официальный телеграм-бот. URL: https://glaz-boga.com (дата обращения: 13.02.2023).

13. Официальный сайт «Демон Лапласа». URL: http://protestonline.ru (дата обращения: 13.02.2023).

14. Официальный сайт Findclone. URL: https://findclone.ru (дата обращения: 13.02.2023).

15. Сервис по поиску архивных копий сайтов. URL: https://web-archive.ru (дата обращения: 13.02.2023).

16. Официальный сайт «Медиалогия». URL: https://www.mlg.ru (дата обращения: 13.02.2023).

17. Официальный сайт компании «Крибрум». URL: https://kribrum.ru (дата обращения: 13.02.2023).

18. Официальный сайт НТЦ «Вулкан». URL: https://ntc-vulkan.ru (дата обращения: 13.02.2023).

19. Поиск комментариев «ВКонтакте». URL: https://vk.com/@11hashtags-poisk-kommentariev (дата обращения: 13.02.2023).

20. Поликарпов Е.С. Основы компьютерной разведки: учеб. пособие. М.: Московский университет МВД России им. В.Я. Кикотя, 2020. 321 с.

21. Принципы работы поисковых систем. URL: https://raiseskills.ru/principy-raboty-poiskovyh-sistem (дата обращения: 13.02.2023).

22. Принципы работы поисковых систем. URL: https://studref.com/380001/psihologiya/printsipy_raboty_poiskovyh_sistem (дата обращения: 13.02.2023).

23. Распознавание лиц и силуэтов людей, автомобилей и номерных знаков NtechLab. URL: https://findface.pro (дата обращения: 13.02.2023).

24. Символы и операторы поисковой строки «Яндекс». URL: https://yandex.ru/support/direct/keywords/symbols-and-operators.html (дата обращения: 13.02.2023).

25. VK.watch – история профилей «ВКонтакте». URL: https://vk.watch (дата обращения: 13.02.2023).

26. OSINT и тестирование методами социальной инженерии. URL: https://www.ntc-vulkan.ru/services/analiz-uyazvimostey/osint-i-testirovanie-metodami-sotsialnoy-inzhenerii (дата обращения: 13.02.2023).

Оглавление

Учебное издание

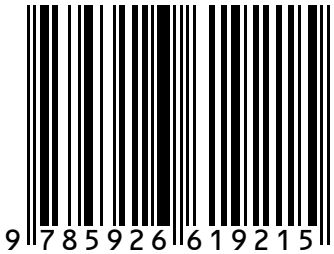
Богданов Дмитрий Сергеевич
Еськов Александр Васильевич

Использование органами внутренних дел специализированного российского программного обеспечения для поиска сведений о физических и юридических лицах в открытых источниках сети Интернет

Учебное пособие

Редактор *В. С. Ревина*
Компьютерная верстка *Г. А. Артемовой*

ISBN 978-5-9266-1921-5



Подписано в печать 28.03.2023. Формат 60x84 1/16.
Усл. печ. л. 4,5. Тираж 70 экз. Заказ 122.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.