МВД России
Санкт-Петербургский университет

Д. И. Якушев, Д. Н. Жидков

КОМПЬЮТЕРНАЯ РАЗВЕДКА

Учебное пособие

Санкт-Петербург
2023

План-график 2023, поз. 45

УДК 004.9
ББК 30
Я49

Якушев Д. И., Жидков Д. Н.

Я49 Компьютерная разведка : учебное пособие / Д. И. Якушев, Д. Н. Жидков — Санкт-Петербург : СПбУ МВД России, 2023. — 88 с.

ISBN 978-5-91837-735-2
EDN UZBVIW

Учебное пособие подготовлено в соответствии с программой дисциплины «Компьютерная разведка». В нем рассмотрены законодательно-нормативные, теоретические и практические вопросы проведения компьютерной разведки органов внутренних дел.

Предназначено для курсантов и слушателей образовательных организаций высшего образования МВД России, обучающихся по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере.

УДК 004.9
ББК 30

Рецензенты:
Арутюнов А. С., кандидат юридических наук, доцент
(Краснодарский университет МВД России);
Дунин В. С., кандидат технических наук
(Дальневосточный юридический институт МВД России)

ISBN 978-5-91837-735-2

ОГЛАВЛЕНИЕ

Знать наперед намерения противника — это, по сути, действовать как Бог!

Сунь-цзы

ВВЕДЕНИЕ

Прежде чем начинать разговор о чем-либо, необходимо договориться о смысле, который мы вкладываем в те или иные термины. В противном случае собеседники просто друг друга не поймут. Смысл термина заключается в его определении — признаках, которые в своей совокупности выделяют объект из окружающей действительности.

В «Википедии» дано следующее определение разведки. Разведка — сбор сведений о противнике или конкуренте для обеспечения своей безопасности и получения преимуществ в области вооруженных сил, военных действий, политики или экономики.

Если не вдумываться, то можно принять и это определение. Однако если соотнести его с деятельностью органов внутренних дел, то где она в этом определении? А если посмотреть шире и вспомнить о разведке полезных ископаемых? Ключевым является понятие «сбор сведений». Однако это не похоже на сбор грибов и ягод. Это ежедневная целенаправленная деятельность, требующая приложения значительных коллективных усилий. Поэтому в рамках настоящего учебного пособия дано следующее определение разведки: разведка — это добыча скрытой информации.

Согласно федеральному закону от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация — это сведения, независимо от формы их представления[1]. Поэтому термины «сведения» и «информация» считаем синонимами.

Когда появилась разведка? Вопрос, видимо, бессмысленный, поскольку разведка — добыча информации — была необходима на всем протяжении существования человеческого общества. Упоминания о ней встречаются в самых ранних письменных источниках. Более того, того разведка есть на только у человека и млекопитающих, но

[1] Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Нормативно-правовые акты приведены в соответствии с данными официального интернет-портала правовой информации Pravo.gov.ru (дата обращения: 20.04.2023).

и у птиц, насекомых (например, пчел). Отсюда следует вывод, что разведка — добыча информации — является деятельностью, возникшей в результате эволюции, и необходима для выживания вида. Одним из первых исторических свидетельств разведывательной деятельности является глиняная табличка, найденная на территории Сирии и датируемая XIII в. до н.э. Текст на ней гласит, что правитель города-государства отпустил соглядатаев, но, согласно договору, выкупа за них не получил.

Компьютерная разведка МВД России — сфера деятельности органов внутренних дел по добыче скрытой компьютерной информации (как скрытой, где скрытой, кем скрытой — здесь не уточняется, поскольку нельзя перечислить все многообразие жизненных ситуаций).

Дисциплина «Компьютерная разведка» является базовой для направления подготовки (специальности) 10.05.05 Безопасность информационных технологий в правоохранительной сфере. Многие представленные в настоящем учебном пособии рассматриваются в дисциплине «Повышение квалификации сотрудников органов внутренних дел Российской Федерации, задействованных в противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий» (тема «Методы киберразведки») и курсе повышения квалификации сотрудников, задействованных в противодействии преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий (тема «Конкурентная разведка в Интернете»).

Целями дисциплины «Компьютерная разведка» являются раскрытие сущности и значения теоретического и практического освоения стандартов и методов применения автоматизированных информационных систем (АИС) в деятельности компьютерной разведки органов внутренних дел, их места в системе национальной безопасности; определение теоретических, концептуальных, методологических и организационных основ обеспечения информационной безопасности; классификация и характеристики составляющих информационной безопасности; установление взаимосвязи и логической организации входящих в них компонентов.

Для того чтобы добывать скрытую компьютерную информацию, нужны инструменты. В контексте рассматриваемой проблематики это программное обеспечение, поскольку условие наличия аппаратного обеспечения (персонального компьютера и сетей связи) компьютерной разведки можно считать выполненным. Под персональным компьютером в настоящем учебном пособии будет пониматься любое персональное устройство, обрабатывающее информацию в двоичном коде.

Необходимым инструментом для проведения компьютерной разведки является специализированное программное обеспечение, которое необходимо либо написать самому, либо использовать уже готовое. В первом случае необходимо не только уверенно программировать, но и в совершенстве знать предметную область: где находится полезная информация и как ее можно извлечь. Такие специалисты ни среди курсантов, ни в рамках дополнительного профессионального образования не встречались. Поэтому остается только один путь — использовать уже имеющееся программное обеспечение.

Общедоступным программным обеспечением являются поисковые системы (наиболее популярные из них — «Яндекс» и Google). Язык запросов этих систем приведен в параграфе 2.3. Опыт преподавания показывает, что только единицы пользуются чем-то более сложным, чем введение поисковых слов через пробел. Насколько известно, специализированное программное обеспечение для компьютерной разведки централизованно не поставлялось. Поэтому на сегодняшний день наиболее доступным широко распространенным инструментом для получения интересующей информации из Интернета является программное обеспечение, за которое во многих случаях надо платить. Одним из примеров подобного программного обеспечения является телеграм-бот «Глаз Бога». Даже в урезанном (Роскомнадзором) варианте это программное обеспечение во многих случаях предоставляет искомую информацию.

В рамках настоящего учебного пособия рассмотрены цели и задачи компьютерной разведки органов внутренних дел, дан обзор использования компьютерной разведки в современном мире, приведены языки запросов поисковых систем «Яндекс» и Google, приведены

ссылки на некоторые сервисы, полезные для проведения компьютерной разведки.

Многие сервисы для проведения компьютерной разведки существуют недолго по различным причинам, в том числе связанным с внешнеполитической ситуацией. Например, многие иностранные сервисы стали недоступны после 22.02.2022 с IP-адресов Российской Федерации. Поэтому некоторые из приведенных в данном пособии ссылок могут оказаться неактуальными уже при его выходе в свет. Как и любая другая сфера деятельности, компьютерная разведка требует времени и внимания. Если какой-то сервис исчез, то на его месте появится новый. Нужно только озаботиться его поиском.

Отдельно стоит обратить внимание на появившиеся с 2021 г. в большом количестве государственные сервисы по предоставлению информации (см. параграф 2.6).

В настоящем учебном пособии описано современное состояние дел в области компьютерной разведки, а также приведены некоторые методы поиска, рекомендации и ссылки на ресурсы, которые могут помочь получению компьютерной информации сотрудниками органов внутренних дел. В рамках данного учебного пособия не рассматриваются методы проведения компьютерных атак, хорошо освещенные в учебном пособии «Компьютерная разведка»[1] и учебнике «Основы кибербезопасности»[2].

[1] Компьютерная разведка : учебное пособие / сост. Е. С. Поликарпов. Краснодар : КрУ МВД России, 2018. — 198 с. URL: https://ebin.pub/c97e8e0d48948a8ae078758aa06291c2.html (дата обращения 24.04.2023).

[2] Винокуров С.А. и др. Основы кибербезопасности : учебник. Воронеж : Воронежский институт МВД России, 2022. — 503 с.

1. КОМПЬЮТЕРНАЯ РАЗВЕДКА ОРГАНОВ ВНУТРЕННИХ ДЕЛ

1.1. Цели и задачи компьютерной разведки

Разведка в компьютерных сетях охватывает процедуры сбора и обработки данных, проводимые с целью их получения из компьютерных сетей. Часто в качестве синонима термина «компьютерная разведка» используется термин «интернет-разведка». При этом как сама информация, так и большая часть программ для ее обработки также доступны через сети связи.

Целью компьютерной разведки органов внутренних дел является добыча оперативно-розыскной информации, зафиксированной в двоичном коде.

Ф. Д. Рузвельт, президент США (1933–1945), назвал разведку «копанием в чужом белье» и высказал мнение, что все задачи разведка должна решать джентельменски, т. е. гласно. Однако после нападения японцев 07.12.1941 на базу Перл-Харбор, когда Америка понесла ощутимые потери, президент вынужден был изменить свою точку зрения.

Игнорирование разведывательных технологий приносит плачевные результаты не только на государственном уровне. Например, после многолетнего доминирования на рынке руководство компании Polaroid назвало отчет аналитического отдела о зарождении цифровой эры футуристической чепухой. Через некоторое время (в 2001 г.) компания Polaroid начала первую процедуру банкротства.

В 1970-х гг. американские производители автомобилей не отреагировали на появление на рынке японской продукции, однако небольшие, экономичные и надежные японские автомобили оказались более востребованными, и американские корпорации понесли значительные убытки.

Разведка корпорации Samsung получила информацию о закрытии последнего американского завода по производству гитар из-за более дешевых корейских инструментов и о том, что правительство США готовится защитить своих производителей с помощью таможенных пошлин. Samsung успела ввезти в США большое количе-

ство гитар, а в результате введения ввозных пошлин — еще и поднять цены на них.

В полевом уставе армии США FM-100-6, содержащем основы информационной войны, приводится иерархия ситуационной осведомленности (рис. 1).

Рис. 1. Иерархия ситуационной осведомленности, согласно полевому уставу США FM-100-6

Ситуационная осведомленность — это восприятие элементов окружающей среды в четырех координатах (3 — пространство и 1 — время), понимание их смысла и прогнозирование их статуса в ближайшем будущем. Иерархия ситуационной осведомленности представляет собой пирамиду, в основании которой лежат данные. На втором уровне находится информация, получаемая путем обработки данных. Изучение информации приводит к формированию знаний (3-й уровень), а логическая обработка знаний приводит к пониманию ситуации (верхний уровень).

Задача компьютерной разведки состоит в получении данных (находящихся в нижней части пирамиды) (см. рис. 1). Анализ этих данных с целью достижения вершины пирамиды — понимания — рассматривается в основном в рамках дисциплины «Информационные технологии в аналитической разведке».

К 1990-м гг. у спецслужб США сформировалось понимание того, что большая часть требуемой информации может быть получена через Интернет с минимальными затратами. Это привело к появлению отдельной статьи расходов на компьютерную разведку. В настоящее время подразделения компьютерной разведки имеются в спецслужбах большинства государств. Перед ними стоит задача проведения легальной разведки в Интернете, организация каналов связи, осуществления информационных воздействий и защиты от них и др. Важнейшая роль в этом отводится разведке, ведущейся в глобальных сетях. Она включает в себя разведку как в открытых, так и в условно открытых источниках, не предназначенных для публикации в средствах массовой информации (СМИ), но доступных в Интернете. Поскольку количество данных огромно, компьютерная разведка немыслима без использования специализированных информационных технологий (IT). Например, для составления сводки объемом в одну страницу ежедневно обрабатывалось 7 млн слов (примерно 15 тыс. страниц).

Значимость разведки по открытым источникам информации отметил еще президент США Л. Джонсон, который в 1966 г. заявил, что высшие достижения не являются результатом потихоньку пересказанной тайной информации, а происходят из терпеливого, ежечасного изучения печатных источников.

По мнению бывшего директора ЦРУ США Р. Хилленкерта, 80 % разведывательной информации получается из таких источников, как книги, журналы, научно-технические обзоры, фотографии, коммерческих аналитических отчетов, газет, теле- и радиопередач. При этом доля затрат на работу с открытыми источниками (например, в разведывательном бюджете США) составляет лишь около 1 %.

По оценке заместителя начальника разведки ВМС США в годы Второй мировой войны адмирала Э.М. Захариаса, 95 % информации разведка ВМС черпала из открытых источников, 4 % — из официальных, 1 % — из конфиденциальных источников. Надо сказать, что часто именно этот один процент являлся недостающим звеном, позволяющим обеспечить понимание ситуации. Представляется, что это соотношение справедливо не только для военной разведки, но и для компьютерной разведки органов внутренних дел.

Основным инструментом проведения компьютерной разведки является персональный компьютер, подключенный к сети «Интернет», что сделало компьютерную разведку доступной не только для небольших компаний, но и для физических лиц. Ничтожность затрат на проведение компьютерной разведки в сочетании с высокой ценностью получаемой информации была оценена по достоинству. Уже в 1999 г. 90 % крупнейших компаний США создали у себя подразделения компьютерной разведки. При этом затраты корпораций на проведение компьютерной разведки составляли 1–1,5 % от оборота и были вполне рентабельны[1].

Развитие этого направления повлекло создание объединений специалистов в области компьютерной разведки (www.scip.org (США), www.competia.com (Канада), www.rscip.ru и www.razvedka-open.ru (Россия). На Украине подготовка специалистов в области компьютерной разведки велась в Харьковском национальном университете радиоэлектроники, где готовят магистров по специальности «Консолидированная информация».

1.2. Разведка на основе открытых источников информации

Практика показывает, что книги, СМИ, консультанты, библиотеки, базы данных во многих случаях не в состоянии конкурировать с Интернетом. При этом 37 % ресурсов Интернета бесплатны, а всего через Интернет предоставляется доступ более чем к 0,6 трлн документов.

Разведка на основе открытых источников (OSINT) — добыча общедоступной информации, которая распространяется среди потребителей, в целях удовлетворения потребностей разведки.

Представленная ниже информация взята из устава ATP 2-22.9 [OPEN] Министерства обороны США, который устанавливает общие понятия, направления и методы сбора данных в компьютерной разведке. Текст адаптирован к потребностям правоохранительных органов.

Открытый источник не требует сохранения конфиденциальности информации. Открытые источники содержат до 95 % информа-

[1] Додонов А. Г. Конкурентная разведка в компьютерных сетях. — Киев : ИПРИ НАН Украины, 2013. — 250 с.

ции, необходимой для достижения ситуационной осведомленности при проведении оперативно-розыскных мероприятий. При этом для достижения максимальной эффективности необходимо использовать результаты компьютерной разведки в комплексе с другими результатами оперативно-розыскной деятельности. Направленность деятельности подразделений *OSINT* зависит от поставленных целей.

Характеристики OSINT:

1. OSINT осуществляется преимущественно на местных ресурсах, которые освещают события и реакцию населения на них.

2. Накопление добытой информации является одной из основной функцией подразделений OSINT.

3. При проведении поиска в Интернете учитываются инструменты и программное обеспечение, используемые в соответствии с политикой подразделения.

4. Критерием отбора данных служат цели и задачи, поставленные перед подразделением OSINT.

5. Получение исчерпывающих сведений о рельефе, климате, геопозиционировании, человеческом факторе и др.

6. Своевременное предоставление как кратких, так и подробных разведывательных справок в рамках поставленных задач. Это, в частности, позволяет проводить корректировку целей и задач, поставленных перед подразделением OSINT.

7. Целью подразделений OSINT является достижение ситуационной осведомленности, что подразумевает прохождение всех этапов от сбора данных до понимания ситуации (см. рис. 1). В числе прочего это подразумевает сопоставление вновь поступивших данных с накопленными.

8. Прогнозирование возможных сценариев развития ситуации, а также своевременного реагирования.

9. OSINT проводится независимо от других мероприятий, проводимых в рамках оперативно-розыскной деятельности.

10. Сопоставление результатов OSINT с информацией, полученной по другим каналам, позволяет достигать понимания ситуации, а также оценивать достоверность имеющейся информации.

11. Тесное сотрудничество в подразделении OSINT способствует повышению эффективность получаемых результатов.

Оцениваются следующие характеристики полученных данных:

— надежность открытого источника;

— достоверность содержания информации;

— соответствие целям;

— мероприятия по обеспечению безопасности;

— гриф секретности;

— координация;

— дезинформация;

— язык сообщения.

Желательные требования к сотрудникам OSINT — наличие технических и культурных знаний, смекалка, предусмотрительность, общественная осведомленность и др.

1.3. Разведка США на основе открытых источников информации

OSINT стала складываться в США с 1947 г.[1] Признаком информационного общества стало возрастание информационных потоков, что явилось одной из причин повышенного интереса к этой области. OSINT проводит добычу и анализ официальных документов, проектов уставов и наставлений, отслеживание новых научных разработок, баз данных, сайтов, блогов и других доступных источников.

Применение OSINT позволяет получить ответы на вопросы, возникающие у военно-политического руководства страны, а также сосредоточить усилия других разведывательных органов на выполнении более сложных и узких задач, не распыляя силы агентурной и других разведок на добывание того, что можно получить из открытых источников. Кроме того, OSINT позволяет получить некоторые данные в случае невозможности для других видов разведки выполнить поставленную задачу.

---

[1] Зенин А. Разведка в сухопутных войсках США на основе анализа открытых источников информации // Зарубежное военное обозрение. 2009. № 5. С. 32–38; Говоров А. Роль открытой информации и тенденции ее использования разведсообществом и Министерством обороны США // Зарубежное военное обозрение. 2012. № 12. С. 26–31.

В США OSINT проводят:

— Управление исследования Вооруженных сил иностранных государств (сбор информации по вооруженным силам России, стран Европы, Азии, Латинской Америки, Китая, изучение новых форм и способов ведения военных операций, включая проблемы асимметричных войн, действий различных террористических организаций и др.);

— Национальное управление геопространственной разведки (картографическое, топогеодезическое и навигационное обеспечение Вооруженных сил США);

— Единое боевое командование США;

— учебные заведения (например, в одном из католических колледжей был сформирован Центр OSINT);

— Азиатский исследовательский институт, решающий задачи в интересах Объединенного командования Вооруженных сил США в зоне Тихого океана;

— ряд других организаций и ведомств.

Общее руководство OSINT в Министерстве обороны США осуществляет заместитель министра обороны по разведке.

Все центры OSINT в США объединены в автоматизированную информационную систему (АИС), информационные ресурсы которой стали называются Intelink-U, в то время как аппаратные средства сети — DNI-U.

Вопрос о необходимости системной OSINT был поставлен в 1992 г. в Сенате США. В 1994 г. в рамках ЦРУ создается управление по реализации этой программы. В 1995 г. это управление выпускает базовый документ — «Стратегический план разведсообщества США по использованию открытых источников информации», где были заложены концептуальные основы современной OSINT. В 1996 г. специальная комиссия Конгресса по оценке роли и возможностей разведсообщества подвергла критике ЦРУ за недостаточное внимание к OSINT. В 2004 г. президент США подписал закон «О реформировании разведки и противодействии террористической угрозе», содержащий указания о включении OSINT в качестве полноценной и равноправной разведывательной дисциплины в деятельность разведки США, а также о формировании Национального центра OSINT. После этого начинается

комплексное системное развитие OSINT (разработка документации, создание организационных и межведомственных структур и др.). Специалисты этого центра ежедневно готовят более 2 тыс. документов (включая переводы, аналитические обзоры, видеоподборки, карты и т. д.), тематика которых охватывает международную политику; военную, экономическую, научную и технологическую сферы; борьбу с терроризмом; контроль за распространением военных технологий; внутреннюю безопасность и др.

В основу действующей нормативной базы OSINT положена директива директора национальной разведки США (2006), которая определяет следующие стратегические задачи:

— принцип «первого шага» — OSINT должна быть «первым шагом» для всех разведывательных дисциплин и предшествовать агентурной разведке и разведке техническими средствами;

— опора на специально подготовленные группы экспертов в области OSINT, обучение методикам добывания открытой информации и внедрение технологий OSINT во все процессы разведывательной деятельности;

— глобальный охват источников информации;

— единая архитектура средств, форм и способов OSINT;

— использование принципа skunkworks (т. е. внедрение для решения отдельных задач передовых методов добычи информации при минимуме бюрократической волокиты).

Директивой устанавливаются правила управления OSINT, проводится разграничение ответственности должностных лиц, определяются необходимая структура и порядок взаимодействия организаций и ведомств разведсообщества США.

Разведданные предоставляются более чем 7 тыс. потребителей (Белый дом, Пентагон, ЦРУ, ФБР, Всемирная информационная библиотека, Европейский парламент, военно-промышленные компании, Coca-Cola, Procter & Gamble, VISA и др.).

В соответствии с нормативными документами сотрудникам разведки запрещается посещение митингов, демонстраций и других мероприятий для сбора сведений без специального разрешения. Существуют четкие правила и при сборе информации в Интернете. Так, со-

трудникам OSINT при сборе информации о гражданах США разрешается использовать только персональные компьютеры на рабочих местах, если другое не определено дополнительно.

В качестве сотрудников OSINT привлекается личный состав резерва Вооруженных сил США. С каждым резервистом подписывается индивидуальный контракт на определенное количество часов работы в месяц, выдается бесплатное аппаратное и программное обеспечение, проводятся шестичасовые online-курсы. При этом выданные персональные компьютеры могут быть установлены в любом удобном для работы и оговоренном в контракте месте, в том числе и дома. Привлекаемые резервисты не получают никакого денежного поощрения, но они могут рассчитывать на благодарность от командования, медали за заслуги и достижения и даже на продвижение по службе.

В OSINT США ведутся исследования, направленные на:

— создание систем многоязыкового перевода;

— выявление в публикуемой в глобальной сети информации скрытых тенденций развития обстановки, связей между разведываемыми событиями, явлениями и объектами;

— использование популярных в Интернете методов организации коллективной работы, накопления знаний, организации социальных сетей, анализа больших данных мультимедийной информации.

1.4. Особенности компьютерной разведки

Согласно действующему законодательству, граждане России вправе требовать от администрации поисковых систем удаления ссылок на недостоверную или неактуальную информацию о себе, содержащую:

— контактные и паспортные данные;

— информацию личного характера;

— информацию, порочащую человеческое достоинство, или не соответствующие действительности сведения, умаляющие честь, достоинство или деловую репутацию гражданина, юридического лица;

— информацию об имеющемся имуществе и финансовом благосостоянии и т. д.

Согласно постановлению Пленума Верховного суда Российской Федерации от 24.12.1993 № 13[1] касательно применения ст. 23 Конституции Российской Федерации ограничение права на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения.

Статья 152 ГК РФ[2] гласит, что гражданин вправе требовать по суду опровержения порочащих его честь, достоинство или деловую репутацию сведений, если распространивший такие сведения не докажет, что они соответствуют действительности.

Статья 5.61 КоАП РФ[3] определяет, что оскорбление, содержащееся в публичном выступлении, публично демонстрирующемся произведении или СМИ, влечет наложение административного штрафа на граждан в размере от 3 до 5 тыс. рублей; на должностных лиц — от 30 до 50 тыс. рублей; на юридических лиц — от 100 до 500 тыс. рублей.

Российское законодательство согласуется с общеевропейской практикой решения аналогичных вопросов.

Живучесть — это свойство объекта сохранять свои основные функции при воздействии внутренних и внешних факторов.

Понятие живучести информации в сети «Интернет» подразумевает потенциальную доступность информации при воздействии дестабилизирующих факторов. Рассмотрим некоторые из них.

1. Создание копии данных на несколько зеркальных серверов при их размещении на хостинге. Например, WikiLeaks использовал несколько сотен серверов, на которых хранились фрагменты копий.

2. Копирование информации пользователями. В зависимости от характеристик информации, количество копий может разниться от нуля до нескольких сотен.

---

[1] Постановление Пленума Верховного Суда Российской Федерации от 24.12.1993 № 13 (ред. от 06.02.2007) «О некоторых вопросах, связанных с применением статей 23 и 25 Конституции Российской Федерации».

[2] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ.

[3] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм., внесенным федеральным законом от 31.07.2020 № 278-ФЗ.

3. Информация в архивах Интернета, например, archive.org. Серверы этого ресурса физически находятся в США и официально принадлежат частному лицу, поэтому убрать оттуда информацию без санкции суда США невозможно. Такое разрешение суд давал лишь дважды. Первый раз — по требованию одной из религиозных организаций, доказавшей, что в архиве находится копия информации, оригинал которой был убран по требованию закона. Второй раз информацию корректировали по требованию правительства, обнаружившего в архиве данные, составляющие государственную тайну. Архив Интернета, расположенный в Сан-Франциско (США), основан в 1996 г. Архив обеспечивает бесплатный доступ для исследователей, историков и школьников. Декларируемой целью архива является сохранение культурно-исторических ценностей цивилизации в эпоху IT и создание интернет-библиотеки.

The Wayback Machine — база данных, в которой можно посмотреть, как выглядел сайт раньше, даже если его больше не существует. В октябре 2004 г. впервые было зафиксировано использование The Wayback Machine в качестве доказательства в суде США. Отмечен случай удаления части архивных копий сайтов, содержащих критику сайентологии, по определению суда.

Библиотека Конгресса США (www.loc.gov) купила права на хранение всех публичных сообщений социальной сети Twitter с 2006 г. и всех твитов, которые будут опубликованы впредь. Библиотека Конгресса также реализует и национальный проект сохранения и распространения цифрового контента Digital Preservation (www.digitalpreservation.gov) (1 400 коллекций данных).

Просмотр ретроспективы сайтов возможен также на:

— wayback Machine;

— archive.today;

— cachedview.com;

— поисковый запрос в Google: cache:website.com.

Для восстановления информации из социальных сетей возможно воспользоваться *https://russia.undelete.news/ru/page/about*.

4. Некоторое время информация остается в кэшах[1] поисковых систем, даже если она удалена с сайта или из социальной сети, откуда она доступна пользователям. У администраторов ресурсов есть возможность удаления своего контента из кэшей Google и Яндекс. Многое о человеке можно узнать из его блога. Социальная сеть Twitter собирает и выдает твиты пользователей. Сервис Google Replay выдает тематические сообщения в блогах.

Для автоматического сбора сообщений предназначены также RSS-агрегаторы. «Яндекс.Лента» и Google Reader копируют информацию сразу после ее размещения. Например, одно из СМИ, связанное с рейдерской атакой осенью 2008 г., удалило информацию на своем сайте через несколько часов после заявления Президента России о том, что рейдеров надо привлекать к ответственности. Однако оказалось, что, кроме «Яндекс.Ленты», эта информация сохранилась на десятках других ресурсов.

5. Информация с сайта может сохраняться на персональных компьютерах конечных пользователей.

Удаление информации с ресурса не приводит к ее удалению из Интернета. Кроме нее, остаются и цифровые следы, и цифровые тени. Цифровой след — информация, которая оставляется самим пользователем при работе в Интернете и по которой можно идентифицировать его и его действия. Часто пользователи добровольно указывают свои Ф.И.О., привязывая дальнейшую информацию к собственной личности, дату рождения, семейное положение, образование, профессию, места предыдущей работы и многое другое, включая контактные телефоны и адреса электронной почты. Цифровая тень — информация о пользователе, создаваемая без его участия:

— кто-то ищет пользователя через поисковые системы;

— пользователь фигурирует в списках электронной почтовой рассылки;

— информация в кэше поисковых машин;

— записи камер наблюдения;

— банковские транзакции;

— биллинги;

[1] Область памяти, предназначенная для временного хранения информации.

— продажа билетов;

— другое.

По оценке аналитической компании IDC, специализирующейся на исследованиях рынка IT, объем цифровой тени уже в 2007 г. превысил объем цифрового следа.

С проблемой репутации в Интернете (негатив в цифровом следе или в цифровой тени) ежедневно сталкивается все больше пользователей. Об этом свидетельствует и предложение услуг по удалению цифровых следов. Так называемые интернет-чистильщики налаживают контакты с администрациями интернет-ресурсов, а также используют специальное программное обеспечение для удаления информации с сайтов и из кэшей. Однако рассчитывать на полное удаление информации не приходится. Лучшим методом оказывается вытеснение нежелательной информации новым контентом: позитивным, правдивым и объективным. Позитивную информацию в сети необходимо размещать на множестве целевых ресурсов, заботясь о ссылках на нее.

Прежде чем начать удалять информацию о себе из Интернета, помните, что:

— удаление информации из Интернета не является ее опровержением;

— удаление своих данных приводит к потере доступа к большинству сервисов, поэтому перед удалением скопируйте их;

— на некоторых ресурсах реализована функция вечного хранения данных;

— иногда проще оставить информацию в покое, чем «поднимать шум» (в 2003 г., когда Б. Стрейзанд через суд потребовала удалить свое фото, количество просмотров изображения было меньше 10, а спустя месяц после подачи иска — почти 0,5 млн).

Удалить информацию о себе из Google можно, заполнив форму «Запрос на удаление незаконно распространяемой, неверной или неактуальной персональной информации из результатов поиска на Google.ru». Удалить личную информацию из «Яндекс»: «Недостоверная, неактуальная информация о гражданине, ссылки на которую подлежат исключению из результатов поиска “Яндекса” (по “Праву на забвение”)». В сложных случаях сделать запрос на удаление лич-

ных данных можно через техподдержку «Яндекс». По статистике, «Яндекс» удовлетворяет 27 % обращений.

Данные в социальных сетях удаляются относительно легко, иногда, однако, только через некоторое время после запроса.

Возможно использовать программное обеспечение для удаления информации, например, deseat.me.

По факту нарушения авторских прав можно обратиться в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор): http://nap.rkn.gov.ru. Однако, скорее всего, в этом случае потребуется судебное разбирательство.

Если вы решили обратиться с проблемой удаления своей информации в специализированную организацию, то, во-первых, гарантий быть не может, во-вторых, вы оставляете свою информацию в этой организации, в-третьих, стоимость подготовки и направления требования об удалении начинается от 10 тыс. рублей, а чистки выдачи в поисковых системах «Яндекс» и Google — от 100 тыс. рублей.

В Лаборатории Касперского подчеркивают, что полностью удалить данные из Интернета нельзя, так как копии этой информации обязательно сохраняются. Поэтому:

— не публикуйте в открытом доступе те данные, с которыми можно вас ассоциировать;

— настраивайте максимальную приватность анкеты;

— не добавляйте неизвестных в друзья;

— выкладывайте в Интернет номер телефона, который нигде более не используется;

— не выкладывайте свои Ф.И.О. и адрес; при необходимости их можно сообщить отдельно по другому каналу связи.

— используйте никнейм;

— помните: все, что вы опубликуете, может быть использовано против вас.

Отметим некоторые особенности компьютерной разведки:

— источников данных должно быть много во избежание опоры на один многократно дублированный недостоверный источник;

— необходимо оценить достоверность каждого используемого источника данных;

— источники данных должны быть независимыми (по крайней мере, контент одного не должен быть копией другого);

— отбор данных должен проводиться в соответствии с поставленной задачей;

— при лимите времени справка может не включать различного рода проверки и аналитику;

— в справке не должно быть ссылок на конфиденциальные источники информации;

— выводы и рекомендации должны быть четкими, краткими и однозначными, а прогнозы носить вероятностный характер, например, в виде совокупности возможных сценариев развития событий[1];

— доведение информации до конечных потребителей должно быть в виде, адаптированном к восприятию заказчика, и форме, легко доступной его пониманию (например, ЦРУ предоставляло президенту США Р. Рейгану ежедневную информацию в виде видеофильма, который снимали каждый день, поскольку бывший киноактер лучше воспринимал такую подачу информации).

1.5. Анонимное распространение информации в сети «Интернет»

Некоторыми сервисами заявляется возможность анонимности точки выхода в Интернет и анонимного размещения информации. Существуют, например, сервисы, предоставляющие услуги хостинга[2] на условиях полной анонимности. Как правило, они располагаются вне России и игнорируют жалобы российских пользователей и ведомств в отношении материалов сайта.

Для выхода в Интернет необходим IP-адрес (от англ. Internet Protocol Address) — уникальный идентификатор устройства. Одновременно не может быть двух компьютеров с одинаковыми IP-адресами.

[1] См.: Якупов Р. А., Якупова Д. В. Прогнозы развития СССР в отражении аналитических материалов ЦРУ США (1981–1991) // Известия высших учебных заведений. Поволжский регион. Гуманитарные науки. 2018. № 1 (45). С. 105–114.

[2] Хостинг — услуга по предоставлению ресурсов для размещения информации в Интернете.

В противном случае будет непонятно, кому из них доставлять данные. IP-адреса выдаются провайдеру[1] специально уполномоченной организацией, а провайдер присваивает эти адреса абонентам. Провайдер — это поставщик услуг связи (т. е. МТС, Мегафон, Ростелеком и др.). Пользователь заключает с ним договор, согласно которому компания предоставляет ему доступ к Интернету. Именно поэтому у провайдера всегда есть доступ к личным данным, которые указаны во время покупки услуг (Ф.И.О., номер телефона, домашний адрес и паспортные данные); всегда можно определить, какому провайдеру и в каком городе принадлежит конкретный IP-адрес.

Установление устройства, с которого осуществлен выход в Интернет, может быть сопряжено со значительными трудностями. IP-адрес может быть статическим, постоянно закрепленным, например, за офисом или квартирой, или динамическим, кратковременно присвоенным подключившемуся к Интернету устройству. Статические адреса обычно платные. Чтобы сменить динамический адрес, достаточно разорвать соединение с Интернетом и установить его заново. Динамические IP-адреса находятся в пределах диапазона, выделенного провайдеру.

Все запросы пользователя в сети «Интернет» попадают на сервер провайдера, так же, как и все ответы. Провайдер видит посещаемые сайты и сохраняет в логах[2] IP-адреса посещенных серверов. Согласно постановлению Правительства Российской Федерации от 12.04.2018 № 445[3] провайдер обязан хранить поисковые данные своих клиентов 30 дней, а согласно п. 1.1 федерального закона «О связи»[4] обязан предоставлять доступ к данным о трафике государственным органам Российской Федерации по запросу. В 2017 г.

---

[1] Интернет-провайдер — организация, предоставляющая услуги доступа к Интернету.

[2] Логи — системные файлы с записями о событиях в хронологическом порядке.

[3] Постановление Правительства Российской Федерации от 12.04.2018 № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи».

[4] Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

в США был отменен закон, согласно которому провайдеры могли передавать личные данные клиентов только по согласию пользователей.

В случае использования https провайдер сохраняет только IP-адрес сервера, время соединения и объем трафика. Адрес сайта и его содержимое в логах не сохраняются. В случае с http провайдер имеет доступ к URL, истории поиска и информации, которую вы просматривали.

В режиме «Инкогнито» браузер не сохраняет историю поиска, но логи у провайдера записываются в обычном порядке.

Если выход в Интернет осуществлялся через публичную точку доступа Wi-Fi, с мобильного телефона, зарегистрированного на подставное лицо, то место выхода в Интернет устанавливается без проблем, но выявление, конкретного пользователя может представлять значительные трудности, поскольку провайдеру при выходе через Wi-Fi становится известен только идентификатор (MAC-адрес) встроенной сетевой карты устройства или внешнего USB-модуля Wi-Fi. Стоимость подобного модуля невысока, поэтому его могут иногда менять. MAC-адрес не шифруется и доступен операторам в полном объеме. Возможно поменять MAC-адрес роутера или персонального компьютера вручную, но это может привести к проблемам с соединением. Поиск пользователя в такой ситуации чаще всего осуществляется путем опроса свидетелей или просмотра записей с камер наблюдения.

Если выход в Интернет осуществляется через GPRS[1] с мобильного телефона или GPRS-модема, у всех пользователей региона адрес одинаковый. Подобное происходит при подключении к Интернету через прокси-сервер[2], подключенный к Интернету с одной стороны и к локальной сети — с другой. Соединение с прокси-сервером не

---

[1] GPRS — «пакетная радиосвязь общего пользования» — надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю сети сотовой связи производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе Интернетом. GPRS предполагает тарификацию по объему переданной/полученной информации, а не по времени, проведенному online.

[2] Сервер — специализированный компьютер для сервисного программного обеспечения. Прокси-сервер — дополнительный сервер, который позволяет защищать устройство от некоторых сетевых атак и помогает сохранять анонимность клиента.

требует установки на персональном компьютере дополнительного программного обеспечения. В общем случае прокси-сервер может скрыть IP-адрес пользователя или заменить его, фиксируя при этом сделанные запросы, посещенные сайты и полученную информацию. Скорее всего, бесплатные прокси-серверы делятся прошедшей через них информацией (они должны на что-то существовать). Располагаться прокси-сервер может в любой стране.

Существует программное обеспечение, предназначенное для сокрытия IP-адресов (анонимайзеры), которое использует прокси-серверы для сокрытия информации об IP-адресе.

VPN (Virtual Private Network — виртуальная частная сеть) — обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети, например, Интернета. Все пользователи VPN и их информация маркируются. Данные защищаются путем шифрования. Для использования VPN требуется установка программного обеспечения и его активация. В результате вместо IP-адреса пользователя отображается IP-адрес VPN. Считается, что использование VPN позволяет:

— обходить запреты регулятора;

— сохранять анонимность;

— сохранять конфиденциальность;

— замаскировать геолокацию;

— перекрывать провайдеру доступ к данным пользователя;

— снизить вероятность утечки и зашифровки информации.

При использовании VPN провайдер видит, что вы отправляете шифрованный трафик на определенный адрес. Он может локализовать этот IP и установить, что он используется для VPN, но отследить, какие сайты вы посетили, провайдер не сможет (при корректных настройках).

При этом:

— если VPN бесплатна, ее хозяева, скорее всего, продают доступную им информацию;

— VPN-сервисы могут передать данные пользователей по решению суда.

В России в 2017 г. вступил в силу закон о запрете на обход блокировок запрещенных сайтов — одной из функций VPN-сервисов. В 2019 г. Роскомнадзор пришел к выводу, что VPN-сервисы эффективнее штрафовать за нарушения, а не блокировать.

В 2013 г. Э. Сноуден рассказал, что АНБ США способно перехватывать VPN-трафик и взламывать практически любое шифрование, в том числе SSH и HTTPS.

1.6. Проблемы компьютерной разведки

В Интернете содержится значительная часть информации, необходимой разведывательным органам, однако остается открытым вопрос ее нахождения и эффективного использования. Причина — присущие сети «Интернет» недостатки:

— высокий уровень информационного шума;

— слабая структурированность и связность информации;

— динамичность информации;

— отсутствие целостности информации;

— отсутствие возможности смыслового поиска;

— ограниченность доступа к «скрытому» Интернету.

Несмотря на это возможности Интернета оцениваются экспертами в области компьютерной разведки довольно высоко.

Центр правительственной связи Великобритании (GCHQ) испытывает серьезные проблемы с наймом и удержанием специалистов по IT. За 2016 г. GCHQ потратил на кибероперации 24 % своего бюджета, а на контртеррористические операции — 23 %. В последние годы GCHQ не в состоянии заполнить штатные вакансии по IT, потому что крупные технологические компании платят в несколько раз больше. Однако для многих специалистов опыт работы в такой организации перевешивает коммерческую выгоду.

Базовое правило компьютерной разведки — собирать информацию там, где предприятие ведет свою деятельность — не всегда выполнимо (например, оказалось, что в Воронежской области всего три интернет-СМИ, из них два — московские); в этом случае выручают контакты с людьми.

Проблемой является доказательство прошлого присутствия документа в Интернете, когда его там уже нет. Иногда удается получить удаленный документ, однако его сложно оформить в качестве доказательства.

Сложности возникают и при некорректной постановке задачи. Здесь необходимо понять интересы заказчика. Иногда ему необходимо разъяснить, что масштаб задачи несопоставим с выделенным бюджетом.

Сложности возникают и при сборе данных на территории вероятного противника. Например, в 2019 г. разведслужбы США объявили конкурс на определение геолокации объектов инфраструктуры в районе г. Мурманска.

Итак, компьютерная разведка открытых источников информации (OSINT) — направление деятельности, позволяющее получать данные из открытых электронных источников. Сбор электронных данных востребован и на государственном уровне, в частности, в США. По имеющимся оценкам, не менее 80 % разведывательной информации добывается из открытых источников. Поэтому не подлежит сомнению, что данное направление деятельности является актуальным и для МВД России.

Вопросы для самоконтроля:

1. Дайте определение компьютерной разведки органов внутренних дел.

2. Нарисуйте пирамиду иерархии ситуационной осведомленности.

3. Оцените количество разведывательной информации, добываемой из открытых источников.

4. Оцените уровень затрат компаний на конкурентную разведку.

5. Дайте определение разведки на основе открытых источников (OSINT). Перечислите цели OSINT. Перечислите используемые в OSINT источники информации.

6. Перечислите факторы, влияющие на проведение OSINT.

7. Кто осуществляет общее руководство проведением OSINT в США?. Какие организации и ведомства проводят OSINT в США?

8. Перечислите стратегические задачи проведения OSINT в США. Кому предоставляются результаты проведения OSINT в США?

9. Дайте определение живучести информации в сети «Интернет». Какие факторы определяют живучесть информации в сети «Интернет»?

10. Что такое IP-адрес? В чем разница между статическим и динамическим IP-адресами? Что такое MAC-адрес устройства?

11. Что такое GPRS? Что такое прокси-сервер? Что такое VPN?

12. Перечислите проблемы проведения компьютерной разведки, которые вам известны.

2. МЕТОДЫ КОМПЬЮТЕРНОЙ РАЗВЕДКИ

2.1. Информационная потребность

Существует несколько сотен определений понятия «информация», но ни одно из них в полной мере не отражает смысла, который в него вкладывается. Поэтому со всех точек зрения удобно использовать определение федерального закона № 149-ФЗ: информация — это сведения независимо от формы их представления.

Во многих случаях удобно разделять понятия «данные» и «информация». Данные — это то, что получено (например, с помощью многочисленных технических систем мониторинга), а информация — это результат обработки данных, который возможно осознать и в дальнейшем применять в своей деятельности.

Потребность — это состояние нужды в определенных условиях жизни, деятельности, материальных и нематериальных объектах, людях или определенных социальных факторах, без которых жизнь затруднена или невозможна.

Эволюцию живых существ нельзя объяснить только приспособлением к среде обитания. Активность более жизнеспособна, чем пассивность. Источником активности живых существ являются потребности. Это функции организма, направленные на приспособление к окружающей среде. Чем больше потребностей, тем выше активность, тем выше конкурентоспособность. Из всех живых организмов, обитающих на Земле, больше всего потребностей у человека. Потребности всегда связаны с наличием у человека чувства неудовлетворенности, которое обусловлено дефицитом того, что требуется. Они определяют объект внимания человека («Голодной куме только хлеб на уме», «У кого что болит, тот про то и говорит»). По мере удовлетворения потребности отрицательные эмоции сменяются положительными.

Одна из лучших классификаций потребностей человека принадлежит, пожалуй, древнегреческому философу Эпикуру (IV–III вв. до н.э.), который разделял потребности человека на три группы.

1. Потребности естественные и необходимые: здоровье, питье, пища, сон, отправление естественных надобностей.

В первую группу входят потребности, необходимые для поддержания жизнедеятельности организма. Сюда же, видимо, можно отнести и потребность во сне.

2. Потребности естественные, но не необходимые: кров, одежда, продолжение рода.

Во вторую группу потребностей входят те, которые проявляются и у других живых существ и не являются необходимыми для поддержания жизнедеятельности организма. Эпикур относит сюда потребность в продолжении рода. Кроме того, видимо, сюда же необходимо отнести потребность в получении информации, поскольку «информационный вакуум» (монотония) одинаково губителен и для человека, и для животных. Даже животные инстинктивно избегают монотонной обстановки. Так, крыса предпочитает использовать в лабиринте разные пути к пище, а не все время один и тот же. Она стремится избежать пространства, в котором провела много времени, и активно ищет менее изученные участки. Таким образом, получение впечатлений об изменениях во внешнем мире, получение информации является (по классификации Эпикура) естественной, но не необходимой потребностью человека, «пищей для ума».

3. Потребности неестественные и не необходимые: роскошь.

В третью группу входят потребности, сформировавшиеся в процессе эволюции сознания, его обособления, что определяет их «неестественность» (они значительно слабее представлены в остальном животном мире). Однако необходимо иметь в виду, что некоторые из потребностей этой группы влияют на способность человека к выживанию в сложившихся условиях. По мере увеличения производительности труда человек все большую часть своего времени и сил направляет на удовлетворение именно этой группы потребностей. Поскольку информация — это то, что осознано, потребность человека в информации необходимо отнести к третьей группе.

Информационная потребность — это желание получения информации. Если причиной возникновения информационной потребности является не любопытство, а деятельность человека, то удовлетворение потребности наступает при получении информации, позволяющей решить задачу, или, по крайней мере, при снижении неопре-

деленности. Показателями, которые используются при оценке деятельности по поиску информации, являются:

— соответствие результатов поиска запросу;

— полнота удовлетворения запроса;

— сжатость и наглядность представления.

При проведении компьютерной разведки, как правило, делается трехуровневая отчетность. Первый уровень — это справка объемом не более одного листа для первого лица. На втором уровне дается сжатое обоснование каждого пункта справки первого уровня. На третьем уровне содержатся документы, послужившие основанием для второго уровня. В справках предпочтительны вероятностные формулировки; в некоторых случаях уместны и парадоксальные формулировки, вызывающие адекватные ассоциации.

2.2. Законодательные основы проведения компьютерной разведки органов внутренних дел

Правовую основу проведения компьютерной разведки составляют Конституция Российской Федерации[1], федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», федеральный закон от 07.02.2011 № 3-ФЗ «О полиции» и другие федеральные законы и принятые в соответствии с ними иные нормативные правовые акты федеральных органов государственной власти.

Считается, что компьютерная разведка подразделяется на гласную и негласную. Законодательной основой проведения гласной компьютерной разведки является п. 4 ст. 29 Конституции Российской Федерации: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». В п. 1 ст. 11 федерального закона «О полиции» говорится: «Полиция в своей деятельности обязана использовать достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру»; в п. 4 ст. 11 — «Федеральный орган исполнительной власти в сфере внутренних дел обеспечивает полиции возможность исполь-

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

зования информационно-телекоммуникационной сети “Интернет”, автоматизированных информационных систем, интегрированных банков данных».

Подразумевается, что основой негласной компьютерной разведки является федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», в котором приведен исчерпывающий перечень допускаемых законом оперативно-розыскных мероприятий. В июле 2016 г. этот перечень был дополнен пунктом «Получение компьютерной информации». Однако до настоящего времени (март 2023 г.) общего юридического понимания этого пункта закона не сформулировано. Существует несколько точек зрения, ни одна из которых не возобладала. Поэтому на сегодняшний день проведение этого оперативно-розыскного мероприятия может осуществляться только на свой страх и риск.

Объектом компьютерной разведки являются данные, находящиеся в двоичном коде, независимо от носителя.

Основаниями для проведения компьютерной разведке согласно ст. 7 федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» являются:

1. Наличие возбужденного уголовного дела.

2. Наличие сведений, ставших известными правоохранительным органам, осуществляющим оперативно-розыскную деятельность:

2.1. Сведения о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, а также о лицах, его подготавливающих, совершающих или совершивших, если нет достаточных данных для решения вопроса о возбуждении уголовного дела (в рамках оперативного дела, для получения достоверной информации; определяются цель, задачи, способы и методы получения информации).

2.2. Сведения о событиях или действиях, создающих угрозу государственной военной, экономической или экологической безопасности Российской Федерации.

2.3. Сведения о лицах, скрывающихся от органов дознания, следствия и суда или уклоняющихся от уголовного наказания.

2.4. Сведения о лицах, без вести пропавших, и об обнаружении неопознанных трупов.

3. Поручения следователя, органа дознания, указания прокурора или определения суда по уголовным делам, находящимся в их производстве.

4. Запросы других органов, осуществляющих оперативно-розыскную деятельность.

5. Запросы международных правоохранительных организаций и правоохранительных органов иностранных государств (в соответствии с международными договорами Российской Федерации).

Условиями проведения компьютерной разведки согласно ст. 8 федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» в рамках оперативно-розыскных мероприятий являются:

1. Судебное решение.

2. Наличие информации:

2.1. О признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно.

2.2. О лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно.

2.3. О событиях или действиях, создающих угрозу государственной, военной экономической или экологической безопасности Российской Федерации.

3. В случаях, которые не терпят отлагательства и могут привести к совершению тяжкого преступления, а также при наличии данных о событиях и действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации, на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, допускается проведение оперативно-розыскных мероприятий, предусмотренных ч. 2 ст. 8 федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», с обязательным уведомлением суда (судьи) в течение 24 часов. В течение 48 часов с момента начала проведения оперативно-розыскного мероприятия орган, его осуществляющий, обязан получить судебное решение

о проведении такого оперативно-розыскного мероприятия либо прекратить его проведение.

4. Допускается только в отношении лиц, подозреваемых или обвиняемых в совершении тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях. Электронная информация, а также ее копии, полученные в результате осуществления компьютерной разведки, хранятся в опечатанном виде в условиях, исключающих возможность их просмотра и тиражирования посторонними лицами.

5. В случае возбуждения уголовного дела в отношении лица результаты компьютерной разведки в соответствии с федеральным законом от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», электронная информация и бумажный носитель (распечатки, отражающие содержание электронной информации) передаются следователю для приобщения к уголовному делу в качестве вещественных доказательств. Дальнейший порядок их использования определяется уголовно-процессуальным законодательством Российской Федерации.

6. В случае возникновения угрозы жизни, здоровью, собственности отдельных лиц по их заявлению или с их согласия в письменной форме разрешается осуществление компьютерной разведки, равно как и прослушивание переговоров, ведущихся с их телефонов, на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность, с обязательным уведомлением соответствующего суда (судьи) в течение 48 часов.

По основаниям, предусмотренным ст. 5 федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности», разрешается осуществлять компьютерную разведку без судебного решения при наличии согласия гражданина в письменной форме.

2.3. Поисковые системы

Поисковая система — комплекс программ, предназначенный для индексации информации и выдачи результатов по поисковым запросам.

Эволюция поисковых систем хорошо представлена в книге К. Шермана и Г. Прайса «Невидимый Интернет»[1]. На русском языке книга не издавалась, но использование онлайн-перевода устраняет это препятствие.

До середины 1960-х гг. связи между компьютерами не было. В 1962 г. была сформулирована концепция глобальной компьютерной сети. Воплощение этой идеи в жизнь в 1969 г. привело к возникновению сети ARPANET, предтечи Интернета. В 1973 г. Министерство обороны США поставило задачу обеспечения надежности связи в условиях разрушительных воздействий на инфраструктуру. Решение было найдено в реализации множества соединений между множеством сетей. Проект назвался Internetting, а сеть из сетей получила название Internet.

По мере роста количества компьютеров в сети возникала необходимость автоматизации поиска информации. При этом подразумевалось, что она в сети есть, но на каком именно компьютере — неизвестно. Решение было найдено в создании специальных компьютеров, предназначенных для удобного обмена файлами — FTP-серверов, которые существуют и сегодня. Первый прототип сегодняшних поисковых систем, основанный на FTP-серверах, появился в 1990 г. Он создавал общий каталог из каталогов, хранившихся на разных FTP-серверах. В 1991 г. было создано программное обеспечение, совмещавшее два протокола — Telnet и FTP, стали использоваться гиперссылки. Этот алгоритм сохранен и по сей день.

В 1993 г. был создан первый web-сканер, названный World Wide Web Wanderer («скиталец» или «странник»). Он просто определял факт существования страницы, не занося ее в свою базу данных. Позднее база данных формировалась.

В 1994 г. был создан сканер WebCrawler (веб-вездеход), который индексировал содержание посещаемых страниц и сохранял результаты в базе данных, которая была доступна по поисковым запросам. В апреле 1994 г. база данных содержала информацию с 6 тыс. серве-

[1] Price G., Sherman C. The Invisible Web: Uncovering Information Sources Search Engines Can't See. Medford : CyberAge Books, 2001. — 430 p.

ров. Ежедневный прирост составлял более 100 новых серверов. Это была первая поисковая система.

В 1996 г. появляется Rambler, в 1997 г. — Yandex, в 1998 г. — Google, в 2004 г. — русскоязычные версии Google и Yahoo!

В состав каждой поисковой системы входят сканеры, которые производят мониторинг сайтов и передают собранные данные на свои серверы. Переход сканера на сайт осуществляется по гиперссылке. Если гиперссылки на сайт нет, он не будет проиндексирован. На сервере поисковой системы текст разбивается на отдельные слова, которые заносятся в таблицу сервера вместе со ссылкой на сайт. Поэтому запрос к поисковой системе предполагает его соответствие словам в индексе поисковой системы. Основное отличие между поисковыми системами заключается в способе расчета релевантности, т. е. степени соответствия выдачи запросу. Поработав со страницей, сканер возвращается на нее, например, через две недели. Если никаких изменений нет, следующее посещение планируется через более длительный период. Если и тогда сканер не обнаружит ничего нового, то «наведается» сюда еще позже. Процесс работы сканеров и последующее сохранение результатов в индексе поисковой системы называется индексацией.

Поисковая система индексирует не все страницы сайта, поскольку стоимость сканирования не должна превышать бюджет. Некоторые ограничивают общее количество страниц в своем индексе, другие — частоту обхода сайтов. Если поисковая система по запросу результат выдает, а попытка перейти на страницу безрезультатна, то, скорее всего, этого сайта уже не существует, но поисковой системе это неизвестно. Третьи ограничивают обход сайтами, которые, как считается, содержат достоверную информацию.

Кроме того, индексация найденных сайтов не всегда возможна:

— на верхнем уровне сайта может находиться файл robots.txt, содержащий список объектов, которые создателя сайта просят не индексировать; большинство поисковых систем «уважают» эту просьбу;

— индексирование сайта может быть запрещено включением инструкции noindex в заголовок документа;

— вход на сайт может быть запрещен паролем (этот метод намного эффективнее, потому что в нем используется технический барьер, а не добровольный стандарт);

— сайт представляет собой форму, состоящую из текстовых полей, требующих ввода пользователем; сама форма может быть извлечена и проиндексирована, но ее содержимое останется невидимым для поисковой системы;

— сканер обнаруживает динамически сгенерированную страницу, признаком которой являются символ «?» в URL-адресе; некоторые из динамических страниц могут вызывать зацикливание сканеров;

— сканер обнаруживает страницу, на которой нечего индексировать;

— сканер сталкивается с сайтом, предлагающим динамические данные в режиме реального времени, например, о прибытии рейсов авиакомпании; с практической точки зрения этот сайт индексировать бесполезно;

— сканер обнаруживает файл .pdf, который технически может быть преобразован в обычный текст, однако это требует времени и средств; индексирование форматов, отличных от HTML, обходится дорого;

— сканер обнаруживает базу данных, предлагающую веб-интерфейс, однако не может проиндексировать данные в силу уникальности ее структуры, инструментов и возможностей поиска и извлечения информации.

Сайты, которые не были проиндексированы, образуют «глубинный» (или «невидимый») Интернет, частью которого является Даркнет.

Подобные сайты, однако, изредка становятся доступны для поисковых систем. Например, 05.06.2018 поисковые системы стали индексировать и выдавать ссылки на документы в Google Docs, содержащие пароли и другую конфиденциальную информацию. Происшедшее стало результатом халатности, проявленной хозяевами документов, которые ненамеренно сделали их доступными для индексации. В компании Group IB рекомендовали защищать свои документы паролем.

Мы ввели адрес сайта и нажали Enter. Что происходит дальше?[1]

Каждый сайт состоит из информации, которая хранится на серверах. Получив адрес сайта, браузер должен понять, к какому серверу обратиться за информацией, т. е. преобразовать адрес сайта в IP-адрес сервера. Для этого браузер определяет, посещался ли этот сайт ранее. Если да, IP-адрес берется из истории, если нет, следует обращение к файлам оперативной системы. Если там адреса нет, следует обращение к недавним адресам в роутере, через который персональный компьютер подключается к Интернету. Если и там нет, то браузер отправляет запрос на DNS-сервер, каждый из которых обслуживает свою часть Интернета. Там точно все есть, но результат получится медленнее. Если нет, идет обращение к другому DNS-серверу. В итоге браузер получает IP-адрес искомого сервера и отправляет по этому адресу запрос на выдачу информации, в котором содержится договор о шифровании.

Когда сервер получает запрос от браузера, он отправляет результат в браузер. Для этого данные нарезаются на пакеты по 8 Кб и нумеруются для корректной последующей сборки. Если пакет данных теряется, происходит повторная отправка. Когда все пакеты собраны, браузер разбирает документ на составляющие: HTML; CSS; JavaScript и др., чтобы построить DOM-модель страницы, которая содержит все элементы и связи между ними. На основе этой модели браузер отображает страницу на экране. Иногда при отображении страницы происходит кратковременная задержка. После загрузки браузер продолжает работать над страницей, выполняя JS-скрипт, подгружая музыку или видео, записывая файлы cookies, а также протоколируя ваши действия.

Поиск информации — одна из самых востребованных на практике задач, которую приходится решать любому пользователю Интернета. Существуют три основных способа поиска информации в Интернете:

1. Указание адреса страницы.
2. Использование гиперссылок.
3. Обращение к поисковому сервису.

[1] Краткий перевод статьи What happens when... URL: https://github.com/alex/what-happens-when (дата обращения 14.01.2023).

Поисковые сервисы могут быть разделены на:

1. Встроенные средства поиска информации на сайтах.

2. Подборки ссылок.

3. Каталоги и поисковые системы (являются базами данных, в которых хранится информация о данных, имеющихся в Интернете). Результатом запроса является список выдачи, содержащий адреса и краткое описание документов, соответствующих запросу. Активировав адрес, пользователь получает оригинал документа. Отличие поисковых систем от каталогов состоит в том, что информация в поисковых системах постоянно обновляется сканерами, а в каталоги информация заносится вручную.

4. Метапоисковые системы (это поисковые системы, сканирующие базы данных поисковых систем). Наиболее известные метапоисковые системы — Vivisimo, MetaCrawler и MetaBot.

5. Системы мониторинга и контент-анализа (сканирование, копирование и анализ информации по заданным темам с заданных ресурсов). Язык запросов подобных систем более развит по сравнению с обычными поисковыми системами. В них, кроме того, реализована функция сохранения прошлых запросов, содержащих сотни знаков. Такие системы хранят в своих базах данных полные тексты исходных документов, что обеспечивает сохранность этих документов во времени. Анализ текстов, реализованный в подобных системах, позволяет устанавливать связи между объектами, оценивать эмоциональную окраску документов, отслеживать хронологию появления документов, выявлять доминирующую тематику и др.

6. Экстракторы (предназначены для выявления в потоке информации объектов, характеризующихся заданными признаками, например, персона, организация, событие, геопозиционирование, отсутствие на автомашине номерного знака установленного образца и т. д.).

7. Системы типа Data Mining, предназначенные для выделения информации (того, что можно осознать) из полученных данных. Востребованность подобных систем на сегодняшний день очень высока, однако, видимо, в силу этого, информации о том, что они могут и насколько хорошо это получается, крайне мало.

8. Системы для проведения компьютерной разведки включают поисковые средства, разработанные для решения поставленных задач. Основной задачей компьютерной разведки является достижение ситуационной осведомленности. На первом этапе производится сбор данных об интересующем объекте. Например, если объектом является физическое лицо, то о нем должны быть собраны данные, находящиеся в двоичном коде (преимущественно в Интернете). Помимо общедоступных сайтов, социальных сетей и ведомственных баз данных государственных органов исполнительной власти (см. параграф 2.6), внимание должно быть уделено и многочисленным негосударственным ресурсам, которые могут содержать интересующие данные. Например, в странах ЕС человек регистрируется в нескольких сотнях баз данных (место жительства, страховка, водительские права, банки, кредитные бюро, информационные, рейтинговые, рекрутинговые агентства, бюро по трудоустройству, медицинские учеты, сетевая торговля, клубы и т. д.). Хранящаяся в базах данных информация о юридических лицах еще более обширна.

9. Интегрированные системы.

Из перечисленных инструментов поиска наиболее известны поисковые системы. Составление запросов к этим системам основано на трех базовых операторах алгебры логики: «И», «ИЛИ» и «НЕ».

1. Использование в запросе логического «И» означает, что в выдаче будут лишь документы, содержащие и то, и другое.

2. При использовании в запросе логического «ИЛИ» в выдаче будут документы, содержащие либо одно слово, либо другое слово, либо оба слова сразу.

3. Если слово в запросе помечено логическим «НЕ», то содержащие это слово документы в выдачу не попадут.

Скобки предназначены для составления сложных запросов. Они раскрываются по правилам математики. Например, выдача на запрос

[апостол И (Петр ИЛИ Павел)]

будет содержать документы, упоминающие либо апостола Петра, либо апостола Павла, либо и того, и другого.

Конструирование запросов во всех поисковых системах основано на этих трех операторах. Синтаксис операторов при этом может разниться.

Язык запросов поисковой системы «Яндекс». «Яндекс» дает воспользоваться инструментарием не с главной страницы — yandex.ru, — а уже после того, как была осуществлена попытка поиска.

Меню «Расширенный поиск» позволяет выбрать регион, в котором вы хотите искать информацию; выбрать период времени размещения информации; задать язык, на котором вы хотите найти данные. Возможно искать картинки, видео, товары, новости, вопросы, услуги, музыку и т. д.

Слова, написанные в запросе со строчной буквы, в выдаче могут быть написаны и с прописной, и со строчной буквы. Слова, написанные в запросе с прописной буквы, будут выдаваться только с прописной.

Логическое «И». В языке запросов «Яндекса» логическое «И» реализуется тремя разными операторами.

1. Вместо оператора «И» в запросе используется обычный пробел. В этом случае в искомом документе слова должны располагаться недалеко друг от друга. В выдаче сначала приводятся документы, содержащие все слова, представленные в запросе, а далее те, в которых на одно ключевое слово меньше.

2. Слова, разделенные в запросе амперсандом (&), в искомом документе должны находиться в одном предложении. Амперсанд должен быть отделен пробелами с обеих сторон.

3. Слова, разделенные в запросе двойным амперсандом (&&), должны присутствовать в искомом документе. Между амперсандами не должно быть пробелов, но сам оператор отделяется пробелами с обеих сторон.

В запросе возможна реализация поиска документов, содержащих слова, находящиеся друг от друга не далее, чем указанно. Для этого используется оператор /n, где n — это максимальное количество слов между словами запроса. Например выдача на запрос [годовой /1 отчет] будет содержать фразу «годовой отчет». Более того, в выдаче будет содержаться и «отчет годовой». В выдаче на запрос [годовой /2 отчет], кроме того, появится «годовой финансовый отчет».

Если в искомых документах допускаются различные варианты написания, то все эти варианты приводятся в запросе в круглых скобках, разделяемых оператором «ИЛИ».

Оператор link в запросе требует, чтобы выдача содержала внешние сайты, содержащие ссылку на сайт, указанный в запросе. Этот оператор часто используется в компьютерной разведке для поиска связей интересующего лица или компании. Этот оператор может сочетаться с обычными ключевыми словами, отделяясь от них двойным амперсандом.

Существует возможность поиска по ключевым словам, расположенным в заголовке страницы (в самом верху экрана).

Другие операторы запросов «Яндекса» представлены в табл. 1.

Таблица 1

Некоторые операторы запросов «Яндекса»

Оператор	Описание	Пример запроса
!	Поиск слова в заданной форме. Допустимо использовать несколько операторов «!» в рамках одного запроса	[!ищущий] — поиск документов со словом «ищущий» в заданной форме
+	Поиск документов, в которых обязательно присутствует слово, перед которым стоит «+»	[годовой + отчет] В выдаче будут документы, обязательно содержащие слово «отчет»
""	Поиск документов, содержащих слова в кавычках в заданной последовательности и форме	[«Во глубине сибирских руд»] В выдаче будут документы, содержащие эту цитату
*	Поиск по цитате с пропущенным словом (словами). Один оператор * соответствует одному пропущенному слову	[«Во глубине * руд»] Будут найдены документы, содержащие данную цитату, включая пропущенное слово

Оператор	Описание	Пример запроса
|	Оператор «ИЛИ». Допустимо использовать несколько операторов | в одном запросе	[эсминец | фрегат] Будут найдены документы, в которых присутствует либо «эсминец», либо «фрегат», либо и то, и другое слово
~	Документы в выдаче должны обязательно включать слово слева от знака, но не должны содержать слово, расположенное справа	«вакуумный ~ насос»
[]	Закрепляет порядок элементов в запросе	_
-	Оператор «-», расположенный перед словом, исключает из выдачи документы, содержащие это слово. Исключаемое слово должно размещаться в конце запроса. Допустимо использовать несколько операторов «-» в одном запросе. Использование оператора «-» перед цифрой будет считаться запросом на поиск отрицательного числа. Чтобы оператор сработал, возьмите слово, начинающееся с цифры, в кавычки	[бал - новогодний]
url:	Поиск по сайтам, размещенным по заданному адресу (URL). Регистр букв в адресе не учитывается. Чтобы найти все документы, адреса которых начинаются с заданного значения, поставьте в конце URL символ *	[искандер url:ru.wikipedia.org/wiki/*] Будут найдены документы, содержащие слово «искандер», адреса которых начинаются с ru.wikipedia.org/wiki
site:	Поиск по всем ресурсам указанного сайта	[искандер site:narod.ru] Будут найдены документы, содержащие слово «искандер» и размещенные на одном из ресурсов сайта narod.ru

Оператор	Описание	Пример запроса
host:	Поиск по сайтам, размещенным на заданном хосте. Идентичен оператору «url:» с заданным именем хоста	[искандер host:www.yandex.ru] Будут найдены документы, содержащие слово «искандер», размещенные на хосте www.yandex.ru
rhost:	Поиск по сайтам, размещенным на заданном хосте. Идентичен оператору host:, но имя хоста записывается в обратном порядке: сначала домен верхнего уровня, затем домен второго уровня и т. д. Для поиска по всем поддоменам в конце URL поставьте символ *	[искандер rhost:com.livejournal.www]
domain:	Поиск по сайтам, расположенным на заданном домене	[искандер domain:ua] Будут найдены документы, содержащие слово «искандер», размещенные на домене ua
mime:	Поиск документов с заданным расширением: pdf, rtf, swf, doc, xls, ppt, odt, ods, odp, odg	[искандер mime:doc] Будут показаны документы в формате doc, содержащие слово «искандер»
lang:	Поиск документов на заданном языке: de — немецкий; en — английский; fr — французский; ru — русский	[искандер lang:ru]

Оператор	Описание	Пример запроса
date:	Поиск документов по дате последнего изменения. Год указывается обязательно, а месяц и день можно заменить символом *	— [фестиваль date:20220224]; — позднее 24.02.2022: [фестиваль date:>20181010]; — в интервале между 24.02.2022 и 10.11.2022 включительно: [фестиваль date: 20220224..20221110]; — соответствует февралю 2022 г.: [фестиваль date:202202*]; — соответствует 2022 году: [фестиваль date:2022*]
cat:	Ограничение области поиска документами, относящимися к указанному региону или рубрике	<текст запроса> cat:<смещенный идентификатор региона или рубрики>
image:	Поиск по названию картинки	image: lol.jpg
title:	Поиск по заголовкам	title:история Windows
Мой ip	Выдает IP Вашего персонального компьютера	–
перевод:	перевод текста (по умолчанию с русского на английский)	–
калькулятор	Наберите в поисковой строке слово «калькулятор». Возможно и просто написать выражение в поисковую строку	–

С операторами языка запросов «Яндекса» можно ознакомиться на странице помощи «Яндекса»[1].

Некоторые дополнительные возможности поиска в «Яндексе».

— меню «Настройки» располагается в нижней части страницы поисковой выдачи;

— историю поиска можно очистить или отключить в настройках.

Язык запросов поисковой системы Google. Google — одна из самых популярных поисковых систем.

[1] Частые вопросы о поиске «Яндекса». URL: http://help.yandex.ru/search/ (дата обращения 24.03.2023).

Особенности поиска Google:

— Google настроен на поиск страниц, на которых ключевые слова расположены недалеко друг от друга;

— все буквы воспринимаются как строчные, независимо от регистра;

— в выдаче Google показан отрывок из текста с выделенными в нем ключевыми словами;

— возможно загрузить страницу по ссылке «Сохранено в кэше» (вид страницы при последнем ее посещении поисковой системой);

— Google не поддерживает морфологию слов; их изначально следует вводить в нужных формах;

— для поиска фразы заключите ее в кавычки: «»;

— количество слов в строке поиска, видимо, не ограничено;

— Кнопка «Мне повезет» расположена на главной странице Google; при ее нажатии Google осуществляет переход на сайт, который поисковая система считает самым релевантным;

— Google распознает как американский (год — месяц — день), так и русский (день — месяц год) формат даты;

— возможно фильтровать картинки по размеру, цвету, типу, лицензии на использование, категории поиска;

— калькулятор (вводите выражение прямо в поисковую строку, причем поддерживаются функции, графики и теоремы;

— если вы знаете номер авиарейса, то просто введите его в поисковую строку, чтобы получить информацию по нему;

— имеется инструмент поиска информации об акциях разных компаний (введите «акции» и название);

— если интересует исключительно тематическая информация о рынках, акциях и ценных бумагах, то проще перейти в этот раздел и производить поиск в нем.

Операторы запросов Google приведены в табл. 2.

Таблица 2

Некоторые операторы запросов Google

Оператор	Описание
Логическое «И» (∧)	Оператор AND, написанный заглавными буквами и отделенный пробелами с обеих сторон: [эсминцы AND фрегаты]
Логическое «ИЛИ» (∨)	Оператор OR, написанный заглавными буквами и отделенный пробелами с обеих сторон: [эсминцы OR фрегаты]
Логическое «Не»	Исключение из выдачи страниц, содержащих слово: [-слово]
+	Поиск документов, обязательно содержащих искомое слово: [+слово]
*	Любое недостающее слово: [годовой * отчет]
«»	Обязательное включение слова в поиск: [«слово»]
AROUND(X)	Выдача документов, в которых между указанными частями фразы будет не более X слов
cache:	Обращение к кэшу. Пробела после двоеточия быть не должно: [cache:www.bstm.ru]
info:	Выдает информацию, известную Google об указанной странице: [info:www.bstm.ru]. Пробела после двоеточия быть не должно
site:	Ограничение поиска конкретным доменом: [site:www.bstm.ru]. Пробела после двоеточия быть не должно
file:	Поиск файлов с заданным расширением: [file:doc]
@	Поиск контента, размещенного в одной из социальных сетей, игнорируя прочие сайты: [@вк]
#	Поиск контента по хэштегу: [#токио2021]
link:	Поиск страниц, которые ссылаются указанную: [link:www.bstm.ru]. Пробела после двоеточия быть не должно
allintitle:	Поиск страниц, в которых все слова запроса содержатся в заголовках (внутри тега Title в HTML): [allintitle: википедия яндекс]
intitle:	Поиск страниц, в заголовке которых содержится слово, расположенное непосредственно после оператора. Остальные слова запроса могут находиться в любом месте текста. Размещение [intitle:] перед каждым словом в запросе эквивалентно размещению [allintitle:] в начале запроса: [intitle: википедия яндекс]
allinurl:	Если запрос начинается с оператора allinurl:, то поиск ограничивается теми документами, в которых все слова запроса содержатся в URL: [allinurl: narod razvedka]. Не работает со специальными символами

inurl:	Слово, написанное слитно с оператором inurl:, будет найдено лишь в адресе страницы Интернета, а остальные слова — в любом месте такой страницы: [inurl:tc razvedka]. Не работает со специальными символами
related:	Выдает страницы, похожие на указанную: [related:it2b.ru]. Пробела после двоеточия быть не должно
define:	Выполняет роль словаря, позволяющего получить определение того слова, которое введено: [define: разведка]
..	Находит все числа внутри указанного диапазона. Прием помогает найти отрезок между датами, модели техники внутри диапазона значений, товары по нужным ценам и т. п.: [20202022]
vs	Находит конкурентов бренда: [Газпромvs]. Без пробела
Feed:	Выдает новости с интересующих сайтов: [Feed: google.com/alerts]
|	Объединяет несколько запросов
lang:	Задание языка
translate:	Автоматический перевод слова

Кроме того, настройки «Инструменты» позволяют:

— ограничивать диапазоны дат, а также использовать команды «before» и «after»; поиск осуществляется не только в поиске, но и в «картинках», и в «новостях»;

— выбрать категории объектов поиска.

Кнопка ⚙ позволяет настроить поиск. Данные в поиске позволяют Google персонализировать дальнейшую выдачу на основании прошлых запросов. Историю поиска можно удалить. В настройках также возможно включить безопасный поиск, выводить больше результатов на странице, отключить показ популярных запросов в меню подстановки и выбрать регион для поиска.

Специалист по информационной безопасности Дж. Лонг собирает поисковые запросы к Google, которые позволяют найти информацию, выложенную в открытый доступ по неосторожности. Например, по запросу:

intitle:»Welcome to Windows 2000 Internet Services»

можно было найти сайты для входа в панели управления «Служб интернета для Windows 2000». А по запросу

allinurl:auth_user_file.txt

можно было найти файлы с логинами и паролями пользователей сайта.

Запросы, подобные этим, Дж. Лонг назвал Google Dorks («dork» переводится как «придурок»).

С июня 2003 г. на сайте exploit-db.com ведется публичная база данных Google Dorks — Google Hacking Database. На 23.01.2021 в ней было 6 267 запросов. Список постоянно пополняется (например, запрос для поиска баз данных в формате xlsx: ext:xlsx inurl:database).

Github Dorks (https://github.com/search) — это поисковые запросы, которые помогают найти приватные данные. Например, набираем в Google: «gmail_password» site:github.com. И на первой же странице поисковой выдачи видим ссылку на документ, в котором есть логин и пароль от Google-почты. Скорее всего, пароль уже неактуален, но если оставить обновления за последние 24 часа, то есть шанс найти действующие пароли. В этом поможет оператор «created:»: extension:sql created:>2021-01-23.

https://twitter.com/obheda12/status/1352686678318731264/photo/1 — один из самых полных списков Github Dorks. В данный момент существует более 500 Github Dorks для поиска различных приватных данных. Например, «db_password», «db_serverd», «b_username», «dbpasswd» дают шанс найти данные для доступа к базе данных; «bx_password», «certificate_password», «ci_deploy_password» ищут пароли; «extension:sql», «extension:sql mysql dump» — ищут дампы баз данных. Некоторые из них можно вводить прямо в поисковой строке Google, добавив «site:github.com». Например:

«cloudflare_api_key» site:github.com

«admin_pass» site:github.com

«api.googlemaps AIza» site:github.com

Используя чужие API-ключи, можно использовать платную функциональность различных сервисов в своих скриптах и приложениях.

Для использования некоторых «дорков» подходит только поиск непосредственно на Github, так как в них применяются специальные операторы поиска: https://github.com/search.

Например, если Github Dorks требует ограничений по используемому языку программирования, то используется поисковый оператор «language:»:

language:javascript

language:python

language:php

Для поиска по именам файлов используется оператор «filename:», а для фильтрации результатов по расширения файлов нужен оператор «extension:».

https://docs.github.com/en/github/searching-for-information-on-github/understanding-the-search-syntax

Полный список поисковых операторов есть в официальной документации Github.

Рассмотрим графическую поисковую систему Quintura Search. При ее использовании возможно выбрать поисковую систему, на которой будет основываться дальнейший поиск, например, «Яндекс». Результаты выдачи сгруппированы по кластерам — сайты с близким наполнением (скорее всего, со скопированной информацией) составляют кластер. Реализована возможность удаления всего кластера из выдачи, что значительно ускоряет ручное рассмотрение выдачи и снижает его трудоемкость. Реализованы дополнительные опции для ручной обработки выдачи, которые удобны в использовании. Однако сама выдача беднее, чем в «Яндексе» или Google. Несмотря на удобство использования пропуск искомой информации представляется недопустимым.

Девиз «Яндекса» «Найдется все!» неприменим к компьютерной разведке, в которой требуется найти только то, что необходимо в соответствии с поставленной задачей. По словам российского эксперта в области компьютерной разведки А. Масаловича, «... из 23 видов поисковых задач, интересующих аналитика спецслужб, “Яндекс” удовлетворительно решает одну»[1].

Можно выделить несколько недостатков универсального поиска:

— выдача поисковых систем, с одной стороны, перегружена бесполезными документами; с другой стороны, в ней отсутствуют

[1] Вебинар на тему: «Как проводить конкурентную разведку в Интернете». URL: https://uralcci.com/news/1958/ (дата обращения 20.06.2023).

необходимые документы, которые, хотя и доступны в Интернете, но не были проиндексированы;

— данные в Интернете меняются, а обращение к архивам Интернета не всегда возможно;

— поисковая система не может отличить важные данные от «шума»;

— поисковая система неспособна анализировать данные с целью получения информации.

Чтобы преодолеть эти недостатки, разрабатываются специализированные поисковые системы. Список некоторых из них приведен по адресу http://hrazvedka.ru/category/poisk_soft. Приведем описание некоторых из них:

— www.softpedia.com/get/Internet/Search-engine-tools-submiting/Website-Finder.shtml — поиск данных на сайтах, плохо индексируемых поисковой системой Google; программа проста в использовании, есть бесплатная версия;

— www.worldin-dustrialreporter.com/solusource — поиск данных в ретроспективных базах данных Thomas (охват — более 100 лет) по компаниям, продуктам и отраслям;

— www.dtsearch.com — быстрый поиск данных, в том числе динамических; реализован поиск во всех форматах MS Office;

— www.strategator.com — программное обеспечение для фильтрации и накопления информации о компаниях из тысяч источников в США, Великобритании и ЕС;

— www.infongen.com — программное обеспечение, настраиваемое на запросы конкретного пользователя, охватывающее более 35 000 источников и предоставляющее информацию на восьми языках;

— visual.ly — поиск графики в Интернете;

— www.quixey.com — поиск ссылок на программное обеспечение, сервисы и расширения для браузеров;

— go.mail.ru/realtime — поиск в mail.ru по обсуждениям тем, событий, объектов, субъектов в режиме реального времени;

— weblib.in.ua — поиск по документам в формате pdf;

— www.zanran.com/q — поиск по документам в форматах pdf, xls, html;

— www.ciradar.com/Competitive-Analysis.aspx — коммерческая англоязычная система поиска данных в «глубинном» Интернете;

— multitender.ru/tenders — поиск по госзакупкам, тендерам и аукционам в России;

— Public.ru — архив СМИ с 1990 г., анализ данных;

— www.rosspending.ru — поиск по российским государственным контрактам на федеральном и региональном уровнях;

— cluuz.com — поисковая система для компьютерной разведки на русском языке; реализован поиск связей между объектами.

2.4. Поиск информации о физических лицах

Пример использования языка запросов поисковой системы «Яндекс» в целях поиска информации о конкретных людях приведен в Е.Л. Ющука «Интернет-разведка: руководство к действию»[1].

Обратимся к запросу данных о Ющуке Евгении Леонидовиче.

Для того чтобы составить такой запрос, в поисковой системе «Яндекс» сначала требуется указать все варианты написания его имени: Ющук Евгений Леонидович, Ющук Евгений, Ющук Е., Ющук Е. Л., а также в иной последовательности: Евгений Леонидович Ющук, Евгений Ющук, Е. Ющук, Е. Л. Ющук. Поскольку слово «Ющук» всякий раз повторяется, а имя или инициалы расположены непосредственно рядом с фамилией, то для «Яндекса» подобный запрос будет выглядеть следующим образом:

[+ющук /1 +(евгений | «евгений леонидович» | «е.л.» | «е»)].

— «+» обозначает, что слово обязательно должно присутствовать в тексте;

— /1 обозначает, что либо непосредственно до него, либо непосредственно после него должен быть текст, описанный далее;

— второй «+» перед открывающей скобкой обозначает, что выражение из скобок обязательно должно присутствовать в тексте;

— | обозначает логическое «ИЛИ».

[1] Ющук Е. Л. Интернет-разведка: руководство к действию. М. : Вершина, 2007. — 256 с.

Если в поисковом запросе «Яндекса» слово написано со строчной буквы, то в документе выдачи оно может быть написано как со строчной, так и с прописной буквы.

Кавычки обозначают цитату.

Затем производится дополнительная фильтрация результатов выдачи: выбираются слова, которые с низкой вероятностью могут встречаться в искомых документах. Априори эту вероятность не оценить, поэтому рекомендуется искать исключаемые слова непосредственно в тексте. Например, в выдачу по Ющуку Евгению Леонидовичу попадает такой текст:

«… Генерал-майор.? 6549. ЧЕРТОК. Абрам. Гершанович. Генерал-майор артиллерии.? 6550…».

При удалении слова «генерал» возможно появление документов, где Ющук Е. Л. упоминается вместе с ним, поэтому стоит найти в тексте слова, которые с наименьшей вероятностью приведут к потере информации.

В частности, документ содержал:

ФЕДЮНЬКИН Иван Федорович Генерал-лейтенант

ФЕКЛЕНКО Николай Владимирович Генерал-лейтенант танковых войск

Возможно исключить документы, содержащие в любом месте текста слова «ФЕДЮНЬКИН» или «ФЕКЛЕНКО», которые являются относительно редкими фамилиями; высока вероятность того, что их удаление из результатов поиска не приведет к потере искомой информации.

При поиске персон за рубежом лучше обращаться к «Белым страницам» (White Pages), которые похожи на телефонный справочник. Например:

[white pages london]

В шаблон требуется внести известные данные человека и получить в выдаче искомые данные. Специалисты отмечают, что на Западе система сбора информации о проживании работает эффективно. Через неделю после вселения в арендованную квартиру человек начинает получать по почте рекламные объявления, адресованные лично ему. Таким образом, «Белые страницы» — достаточно ценный ресурс, поддерживаемый в актуальном состоянии.

«Яндекс.Метрика» — бесплатный сервис для оценки посещаемости сайтов и анализа поведения пользователей.

Social Mapper — программное обеспечение с открытым исходным кодом для поиска связей между профилями в социальных сетях через распознавание лиц.

Knowem — бесплатный сервис для проверки по никнейму в 400 социальных сервисах и 40 доменных именах.

SpiderFoot сбор данных со 100 открытых источников по IP-адресу или доменному имени. В отличие от Maltego, интерфейс SpiderFoot доступен в браузере. Для анализа данных, которые собираются в офлайн-режиме, а не из открытых источников, необходимо использовать CaseFile.

Сервис проверки почт на «слитые» пароли: https://leakcheck.io/. Пароли в основном крадутся вирусами, которыми заразилось устройство. Создатели вирусов продают или просто выкладывают базы даных собранных паролей с почтами или логинами на различные форумы. А сайт leakcheck либо покупает эти базы данных, либо мониторит форумы, на которых они могли появиться. Телеграм-бот mailsearch_bot может проверять, появлялся ли когда-нибудь пароль от почты, логина, номера телефона (только СНГ) в открытых источниках, или, наоборот, показать логин по паролю. После регистрации есть 100 бесплатных проверок. Например, по E-mail kirill007@mail.ru найдено 17 паролей, окончания которых заменены на звездочки. Количество звездочек равно количеству символов, поэтому символы в некоторых случаях возможно восстановить. Например, одиннадцать цифр, начинающихся с восьмерки — это номер телефона. Пароль ufkjlyst****: если поменять раскладку клавиатуры, то получится галодные****, из-за популярности фильма можно предположить, что «голодныеигры». Пароль rbhbkk***: скорее всего, это «кирилл***». Если приобрести подписку (160 руб./сутки), то все пароли будут показаны в полном объеме.

Для поиска информации о физических лицах возможно использовать следующие сервисы:

1. «Яндекс» (в 2020 г. поиск «по людям» был встроен в основной поиск: https://yandex.ru/people). Добавляйте к поисковому запросу VK («ВКонтакте») или аббревиатуру другой социальной сети. Сервис

предоставит вам выборку, которая обрабатывается вручную. Для поиска возможно использовать никнейм.

2. Сервис для поиска контактов корпоративной почты Email Finder: https://snov.io/ru/.

3. Бесплатный сервис для поиска в социальных сетях по ключевому слову Social searcher: https://www.social-searcher.com/

4. Социальные сети лучше проверить вручную: «ВКонтакте» — https://vk.com/search; «Одноклассники» — https://ok.ru/; «Мой Мир» — https://my.mail.ru/; «Фейсбук» — https://www.facebook.com. Можно искать по E-mail или телефону. При отсутствии результатов поищите друзей и родственников человека. Перейдите на английскую версию, где, возможно, больше инструментов для поиска. Используя геопозиционирование, поищите место, где человек проводит время. Попробуйте начать процедуру восстановления забытого пароля, указав тот же E-mail. Возможно, вы найдете страничку, фото или имя учетной записи.

Если профиль в социальных сетях открыт, можно сделать выводы о графике передвижений владельца (примерное время публикации постов), материальном положении (домашние селфи), проживании и месте жительства (геолокация), круге общения.

Инструменты поиска геолокации в социальных сетях приведены в табл. 3

Таблица 3

Поиск по геолокации в социальных сетях

Среда	Инструмент
YouTube	mattw.io/youtube-geofind/location montage.meedan.com/welcome
VK	vk.com/feed?section=search snradar.azurewebsites.net photo-map.ru
Twitter	twitter.com/search-advanced twimap.com
Snapchat	map.snapchat.com
Instagram	osintcombine.com/instagram-explorer instmap.com
Facebook	whopostedwhat.com
Прочее	intelx.io/tools?tab=location

В Stories можно узнать, что человека нет дома.

Если профиль закрыт, дата рождения, место учебы и работы все равно доступны. С этой информацией можно продолжить поиски на других сайтах. К тому же, если близкие регулярно делятся фото, то они доступны.

Сервис упоминаний о человеке в социальных сетях: Social Mention: http://socialmention.com/

Сервис поиска постов в социальных сетях: Social Searcher: https://www.social-searcher.com/

Если человек есть в социальных сетях, можно обратиться к нему напрямую. Возможно обратиться и к его друзьям. Если же друзья не дают его контакты, то можно попросить передать информацию.

Можно осуществить поиск человека по возрасту, городу, школе, соседям, увлечениям.

Сайт www.nomer.org позволяет искать информацию по телефонным справочникам ряда городов СНГ. Здесь по телефону, адресу или фамилии, имени, отчеству можно получить дополнительную информацию в отношении искомого лица и его связей.

Особенности поиска в GetContakt:

— подтверждение имени и фамилии;

— следует обращать внимание на сопутствующие иконки;

— возможно указать место работы и другие характеристики.

5. Используйте поисковые системы «Яндекс» и Google. Запрос может содержать фамилию, имя, номер телефона, E-mail. Воспользуйтесь оператором «OR». Сформируйте сложный запрос, например, [!Евгений & !Ющук && !»*.05.1963»], где * — любая дата. Попробуйте транслитерацию на латинице имени и фамилии, в кавычках и без.

6. Для исследования ретроспективы сайта воспользуйтесь архивом: http://web.archive.org/.

7. Извлеките IP-адрес отправителя E-mail: откройте оригинал письма, IP-адрес находится в квадратных скобках в строке «Received». Уточните его местоположение: https://ru.infobyip.com/ или https://ip2.ua.

8. Поищите в Skype, Viber, Telegram, ICQ и др. Занесите номер телефона к себе в контакты: возможно, вы получите фото.

9. Произведите поиск по фото, например, https://ocomp.info/kak-nayti-cheloveka-po-foto.html.

10. По номеру телефона начните перевод средств — вы узнаете имя, отчество и первую букву фамилии.

11. Поиск на сайтах образовательных организаций (школы выкладывают списки выпускников, вузы — списки поступающих).

12. В качестве инструментов для проведения компьютерной разведки рекомендуют:

— https://start.me/p/DPYPMz/the-ultimaye-osint-collection;

— https://start.me/p/ELXoK8/bellingcat-osint-landscape.htm (не работает (08.04.2022), возможно, только с российского IP);

— https://urlscan.io/PDFCandy (не работает (04.04.2022), возможно, только с российского IP);

— https://pdfcandy.com/WiGLE (не работает (04.04.2022), возможно, только с российского IP);

— https://www.wigle.net/PublicWWW (не работает (04.04.2022), возможно, только с российского IP);

— https://t.me/DarkSidePlanets/18 (база данных по поиску людей (около 600 Гб) — через Telegram;

— https://xinit.ru — поиск по номеру сотового телефона;

— https://publicwww.com;

— https://www.найти-телефон.com;

— https://www.avtobot.net — поиск информации о владельце автомобиля по номеру;

— https://www.ibestresume.ru/resources — множество дополнительных сервисов.

2.5. Поиск информации о юридических лицах

Визитной карточкой компании в Интернете является ее корпоративный сайт. Практически всегда помещенная на сайте информация о месторасположении, должностных лицах и банковских реквизитах организации соответствует действительности.

Поиск сайта компании, адрес которого неизвестен, начните с ввода названия организации в запрос Google и анализа первой страницы результатов выдачи. Если результат отрицательный, попробуй-

те изменить запрос, используя номера телефонов, имена людей, электронной почты, физические адреса. Попробуйте использовать другие поисковые системы.

Основную информацию о сайте можно узнать через сервис Spyonweb. Он показывает IP-адрес хостинга, идентификатор для сервиса аналитики, данные о DNS-серверах. Проверить данные о регистрации можно на сайте DomainBigData — туда выводится имя регистратора, дата и другая информация. Посмотреть сохраненные копии сайтов или заархивировать их можно через Internet archive и Archive.is.

Чтобы проверить, на кого зарегистрирован сайт компании, пользуются ресурсом nic.ru. Возможно проверить и свой сайт, чтобы убедиться, что у него статус «Занят». Чтобы посмотреть историю, нажмите «Whois» → «История Whois для домена *.*». Владелец сайта указан в строке «Org:». Там же есть разбивка по периодам.

Используйте поиск в Google, например: site:mgma.com inurl:members. Mgma.com — это сайт компании, причем URL-адрес содержит слово «members».

Зайдите на сайт компании в разделы «О нас» или «Команда»; найдите список участников какого-нибудь мероприятия. Далее используйте социальные сети: в Twitter есть расширенный поиск; можно использовать сервис Foller; для поиска в Facebook можно использовать сервис Inteltechniques, позволяющий сконструировать запрос. Список поисковых формул собран на сайте Plessas, для поиска в VK можно использовать сайт Vkpt.

Платные ресурсы. Компания Dun&Bradstreet (www.dnb.ru и www.dnb.com) работает с 1841 г. Dun&Bradstreet выходит на контакт с изучаемой компанией и прямо просит предоставить о себе информацию. В случае отказа ей говорят, что непредъявление сведений — ее законное право, однако в таком случае в соответствующей графе будет сделана запись об этом отказе, что для любого предприятия автоматически означает катастрофическое падение доверия со стороны инвесторов.

Обращение к специальным сервисам позволяет получать информацию о предприятиях. Часть этой информации находится в свободном доступе, часть предоставляется на платной основе:

— сайты, посвященные вопросам безопасности: www.oxpaha.ru, www.it2b.ru, www.sec.ru и www.agentura.ru;

— проверка доменного имени с использованием различных сайтов (например, www.check.ru) позволяет установить, на чье имя и в какой стране зарегистрирован сайт, иногда указываются телефон и адрес владельца сайта;

— www.lin.ru — законодательство и инвестиции;

— www.valaam-info.ru (ВАЛААМ): сведения из ЕГРЮЛ и ЕГРИП; учредительская деятельность юридического лица; аффилированные лица;

— www.cbr.ru — сайт Банка России;

— www.spark.interfax.ru (СПАРК): сведения из ЕГРЮЛ и ЕГРИП (сведения из ЕГРЮЛ доступны бесплатно); балансы; арбитраж; банкротства; новости компаний. disclosure.interfax.ru: эмитенты, аффилированные лица (бесплатно);

— www.scrin.ru (СКРИН): сведения об участниках рынка ценных бумаг, подлежащие раскрытию (бесплатно);

— www.disclosure.ru: сведения об участниках рынка ценных бумаг, подлежащие раскрытию (бесплатно);

— www.nalog.ru — сайт ФНС России (с некоторых пор на нем стало возможным часть информации получать бесплатно).

Полезную информацию также можно найти на сайтах Счетной палаты России, Высшего Арбитражного суда, Федеральной регистрационной службы, Базы эмитентов акционерных предприятий, Федеральной службы по финансовым рынкам и др. Анализ этой информации позволит получить установочные данные на интересующее юридическое лицо (дату, адрес регистрации, ИНН, ОГРН), а иногда данные и о составе правления, руководителе, акционерах, главном бухгалтере и др. Переход на многие из вышеуказанных бесплатных ресурсов для удобства специалистов предусмотрен на сайте http://ci-razvedka.narod.ru.

Воспользуйтесь «Желтыми страницами» — справочником компаний, сгруппированных по видам деятельности, например,

[«желтые страницы» екатеринбург] или

[портал екатеринбург].

Там же можно найти информацию об иностранных компаниях. Кроме того, можно воспользоваться:

— www.companieshouse.gov.uk (Великобритания);

— www.infoimprese.it (Италия);

— www.kvk.nl (Нидерланды);

— www.justice.cz (Чехия);

— www.infogreffe.fr (Франция);

— www.ytj.fi (Финляндия).

На сайте http://ci-razvedka.narod.ru приведены ссылки на европейские поисковые ресурсы (некоторые из них используют собственные сканеры для индексации тематических разделов Интернета, но делают это полнее, чем универсальные поисковые системы).

Для улучшения результатов поиска используются следующие методы:

— изменение критериев поиска;

— изменение правописания и грамматики;

— транслитерация;

— использование синонимов;

— поиск в кэше;

— поиск в архивах;

— поиск по URL;

— усечение URL до слэша;

— домены сайтов.

Поиск информации о предпринимателе по Ф.И.О.: www.focus.kontur.ru.

Сотрудники ФНС России стали активно использовать при проверках информацию из Интернета: данные с сайтов компаний, их контрагентов, ресурсов по поиску работы, социальных сетей и т. д. Сначала изучается IP-адрес сайта на сервисах bname.ru, pr-cy.ru или ip-whois.net/website_ip.php. Проверяется, какие еще сайты имеют тот же IP-адрес. Сведения об общих IP-адресах или о прежних владельцах сайта используются для доказательства взаимозависимости компаний. Это повод, чтобы пересчитать налоги по спорной сделке или взыскать налоговые долги с взаимозависимого юридического лица. Активность компании в Интернете и посещаемость сайта сопостав-

ляются с финансовым результатом компании. Ежедневное обновление новостей, сообщения об удачных проектах и отражение в отчете убытков — повод заподозрить компанию в занижении налогов. Отмечаются и негативные отзывы на сайте, например, о завышении цен, и одновременные убытки в отчетности. Сведения о компании, ее руководстве и контактах сравниваются с данными из ЕГРЮЛ. Наличие адресов дополнительных офисов на сайте, по которым компания не зарегистрировала обособленные подразделения, грозит штрафами. То же касается видов деятельности, не указанных в ЕГРЮЛ, или ассортимента, которого нет в учете. В качестве доказательств используются скриншоты с сайта компании. Интересует проверяющих и раздел вакансий. Зарплаты из объявлений сопоставляются с окладами по штатному расписанию. Более высокие обещания свидетельствуют о зарплатах в конвертах. Раздел о партнерах используется для доказательства искусственного усложнения схемы поставки.

Не только сотрудники ФНС, но и трудовые инспекторы, и другие специалисты изучают сайты по поиску работы на предмет нестыковки между объявлениями о вакансиях и зарплатами в компании. Наиболее популярные ресурсы: https://hh.ru, https://superjob.ru, trudvsem.ru, rabota.ru, zarplata.ru. Проверяется информация о вакансиях и в социальных сетях, например, на https://vk.com/moscow_rabota. Доказательством серой зарплаты будет скриншот объявления с обещанием более высокого оклада. Ревизоры могут обвинить компанию в занижении базы по страховым взносам и неполном удержании НДФЛ, а физическое лицо — в сокрытии доходов. Суды принимают такие доказательства и поддерживают доначисления (постановление Арбитражного суда Западно-Сибирского округа от 07.10.2015 по делу № А27-3089/2015)[1]. На сайтах с отзывами проверяющих интересует негативная информация о компании, причем не только как о продавце или покупателе, но еще и как о работодателе (например, то, что клиентам не выдают документы, занижают цены, не пробивают кассовые

[1] Постановление Арбитражного суда Западно-Сибирского округа от 07.10.2015 по делу № А27-3089/2015 // Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/arbitral/doc/8IIKPhSvRKdJ/ (дата обращения: 12.01.2023).

чеки, а сотрудники получают серую зарплату). Трудовые инспекторы ищут комментарии о задержках по зарплате, работе без оформления и других нарушениях прав работников.

Ревизоры изучают отзывы и о контрагентах компании. Единичные отзывы указывают, что партнер — «однодневка». Тогда они могут снять расходы и вычеты по сделке. Когда есть и другие признаки неблагонадежности, суды поддерживают инспекторов (постановления Девятого арбитражного апелляционного суда от 24.08.2017 по делу № А40-16084/17[1], от 29.12.2016 по делу № А40-99755/16[2] и от 19.02.2015 по делу № А40-128809/14[3]).

Большая база отзывов доступна на «Главном форуме потребителей России» (forum.ozpp.ru). Отзывы о работодателях по всем регионам есть на сайтах orabote.top, antijob.net, pravda-sotrudnikov.ru и др. На сайте orabote.top также размещены рейтинги работодателей, например, «Суда нэ хады» — самые низкорейтинговые компании, «Туда хады» — самые рейтинговые компании, «Вы популярны» — самые просматриваемые компании. Скриншоты с подобных сайтов не доказывают налоговые нарушения, но могут стать поводом для более детальной проверки. Если автора отзыва можно идентифицировать, налоговики вправе допросить его как свидетеля и использовать полученные показания в суде (пп. 12 п. 1 ст. 31 и ст. 90 Налогового кодекса Российской Федерации[4]).

Инспекторы используют социальные сети, чтобы найти и оштрафовать незарегистрированных предпринимателей, о чем пре-

---

[1] Постановление Арбитражного суда Западно-Сибирского округа от 07.10.2015 по делу № А27-3089/2015 // Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/arbitral/doc/Ya9SW1YdmR1q/ (дата обращения: 12.01.2023).

[2] Постановление Арбитражного суда Западно-Сибирского округа от 07.10.2015 по делу № А27-3089/2015 // Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/arbitral/doc/8FdcQTlK6e1S/ (дата обращения: 12.01.2023).

[3] Постановление Арбитражного суда Западно-Сибирского округа от 07.10.2015 по делу № А27-3089/2015 // Судебные и нормативные акты Российской Федерации. URL: https://sudact.ru/arbitral/case/iacvCEzfKQJX/ (дата обращения: 12.01.2023).

[4] Налоговый кодекс Российской Федерации от 31.07.1998 № 146-ФЗ.

дупреждают сами, например, УФНС России по Мурманской области (URL: nalog.ru/rn51/news/activities_fts/6984434/). Признаками нарушений являются реклама услуг, продвижение товаров и др. Такую информацию из социальных сетей суды принимают как доказательство нарушения (постановление Арбитражного суда Северо-Западного округа от 02.12.2014 по делу № А05-808/2014[1]). Публикации в Интернете можно найти через сервисы google.com/alerts?hl=ru, sitesputnik.ru, iqbuzz.pro, youscan.io и др. Некоторые из подобных ресурсов платные.

Есть сайты, дающие доступ к объявлениям *Avito* по номеру телефона. По ним можно составить представление о месте жительства человека, а иногда и о его доходе, например, если он продал квартиру. Сайт mirror.bullshit.agency выдает старые объявления на сайте Avito.

Считается, что при использовании поисковых систем можно найти только 25 % необходимой информации. Остальные 75 % содержатся в так называемом Deep Web, который не индексируется. Добывание этой информации требует уровня продвинутого пользователя. Ресурс OSINT Framework содержит ссылки на коллекцию ресурсов для компьютерной разведки — от сбора адресов E-mail до поиска в социальных сетях и даркнете.

Возможно применение инструментов для поиска подключенных к Интернету устройств, например, через поисковую систему Shodan, которая позволяет провести качественную аналитику по вопросам безопасности, проверить уязвимые места конкретной цели (открытость личных данных, доступной паролей и портов, IP и т. д.).

Для проведения компьютерной разведки существует много ресурсов (большинство из них англоязычные, некоторые платные, а некоторые существуют менее года). Например: https://pipl.com, https://www.spokeo.com, https://thatsthem.com, https://www.beenverified.com, https://www.fastpeoplesearch.com, https://www.truepeoplesearch.com, https://www.familytreenow.com, http://www.pipl.com, http://ark.com, http://waatp.com, http://findpeopleonplus.com, http://fotki.yandex.ru, http://www.poiski.ru, http://zopeo.com, http://www.spokeo.com,

[1] Судебные и нормативные акты Российской Федерации. URL:https://sudact.ru/arbitral/doc/xx90vzqYQSmw/ (дата обращения: 12.01.2023).

http://www.cvgadget.com, http://ru.kgbpeople.com, http://trap.it, http://yoname.com, http://www.tweenme.net/login.php, http://www.picslikethat.com, http://www.googleimageslideshow.com, http://www.facesaerch.com. Русскоязычных бесплатных сайтов, которые существуют более года, не так много, например, https://people.yandex.ru.

Сбор информации через метапоисковую систему Searx, позволяющую собирать данные анонимно из более чем 70 поисковых сервисов.

Отслеживание местоположения человека по его фотографиям в социальных сетях, например, через сервис GeoCreepy.

Сервис Metagoofil использует поисковую систему Google для извлечения общедоступных файлов .pdf, .doc, .ppt и .xls из заданного домена.

Возможно применение Open Source Intelligence Browser Extension; изучение служб DNS, доменов, поддоменов и IP-адресов; применение иных инструментов Kali Tools.

Метод поиска от Е.Л. Ющука.

1. Перейдите на сайт интересующей организации.
2. Получите адрес любого изображения с этого сайта.
3. Укоротите его до последнего слэша справа.

Если перейти по полученной ссылке, появится запрос по авторизации. А если ввести эту ссылку на ресурсе Web ThumbnailExpert, запрос не появится.

Yatedo.com — ресурс по поиску людей, в профиле которых указано название интересующей компании. Например, при поиске по «полиция Нью-Йорка» вы получите значительное количество результатов, около 20 % из которых будут содержать фото. А при поиске по «авиакомпания Transaero» фото будет уже в 60 % выдачи.

2.6. Некоторые методы поиска информации

Браузер сохраняет в памяти ваши запросы, что позволяет работать быстрее. Сохранение также работает и с адресами E-mail, и с паролями. В настройках браузера эти данные доступны. Доступ в Google Chrome: Настройка → Автозаполнение → Пароли; в Mozilla Firefox: Настройки → Конфиденциальность и безопасность → Логины и пароли → Сохраненные логины.

Просмотр сайтов, открывавшихся на персональном компьютере после удаления истории просмотра (операционная система *Windows*), независимо от того, был использован приватный сеанс просмотра или нет:

1. «Выполнить» (Win + R или «Пуск» → «Выполнить»).

2. Вводим cmd и нажимаем Enter.

3. В командной строке вводим: ipconfig/displaydns, Enter.

На экран выведется список посещенных сайтов.

Можно также сделать восстановление системы из копии или синхронизации данных браузера с облачным сервисом.

Сервис Google Alerts (тревога): https://www.google.ru/alerts# позволяет узнать, что вас кто-то ищет в Интернете. Для доступа к большему количеству функций заведите аккаунт на Gmail. Обратите внимание, что некоторые запросы в кавычках, а другие — нет. «Яндекс.Медиана» — это аналог Google Alert для поисковика «Яндекса».

Как посмотреть пароль от Wi-Fi в Windows:

1. Нажмите правой кнопкой по «Пуску» и выберите «Сетевые подключения».

2. Далее зайдите в «Настройка параметров адаптера».

3. Там найдите свой адаптер беспроводной сети: «Беспроводная сеть» или Wireless в описании адаптера.

4. Нажмите на него правой кнопкой и выберите «Состояние».

5. Зайдите в «Свойства беспроводной сети».

6. Зайдите во вторую вкладку: «Безопасность».

7. В пункте «Отображать вводимые знаки» поставьте галочку и чуть выше вы увидите пароль от Wi-Fi.

Регистрация в сервисах осуществляется по письмам со схожим оформлением и содержанием. Поэтому при вводе поискового запроса subject: verify отобразятся все письма, в теме которых встречается слово verify.

Основные способы взлома паролей[1]:

— BruteForce пароля — перебор всевозможных комбинаций.\;

[1] URL: https://tproger.ru/articles/vzlom-wi-fi-sposoby-i-programmy/ (дата обращения 07.02.2023).

— взлом WPS (Wi-Fi Protectes Setup) — подбор пароля из 8 цифр или взлом стандартных заводских PIN-кодов из приложений баз данных;

— беспроводные адаптеры, актуальный список которых можно посмотреть на https://hackware.ru/?p=6780;

— фишинг — метод, при котором данные для входа пользователь вносит сам; это можно реализовать самостоятельно либо с помощью приложения для взлома Wi-Fi Wifiphisher: https://github.com/wifiphisher/wifiphisher;

— взлом роутера (сработает, если вы можете подключиться к Wi-Fi по проводу или знаете внешний IP-адрес; в этом случае можно попытаться подобрать логин и пароль к роутеру; часто они остаются заводскими по типу admin/admin; пароль же от Wi-Fi будет лежать в настройках).

Kali Linux и взлом Wi-Fi. Kali Linux содержит более 300 утилит для тестирования информационной безопасности, некоторые из них дублируются. Возможна установка и стороннего программного обеспечения для взлома Wi-Fi. Подробнее о Kali Linux: https://www.youtube.com/watch?v=T0qeXWq0uFk&t=17s.

Для получения root-прав пропишите в командной строке: sudo passwd и задайте пароль. Затем перезагрузите компьютер и зайдите под логином root, чтобы в дальнейшем не приписывать к каждой команде sudo.

Обновите операционную систему: apt update && apt upgrade –y.

Установите систему контроля версий Git: apt install git –y.

Также советуют установить:

— Atom — текстовый редактор для работы с кодом: https://github.com/atom/atom/releases;

— Double Commander — аналог Total Commander для Linux с большим количеством полезных функций;

— Filezilla — для работы с FTP, SFTP, и FTPS;

— Network Manager OpenVPN — графический интерфейс для настройки VPN;

— Tor Browser лучше скачать с официального сайта: https://www.torproject.org/; добавьте репозитории Tor Project в список APT, загрузите ключ подписи пакета и импортируйте в APT-ключ.

Под Kali Linux рекомендуют также программное обеспечение Airgeddon, не требующее специальных навыков.

Более сложные инструменты в рамках данного учебного пособия не рассматриваются:

— Fern Wi-Fi Wireless Cracker — бесплатное программное обеспечение для аудита беспроводных сетей;

— WepDecrypt — бесплатное программное обеспечение для взлома сетей, защищенных протоколом WEP;

–Wifiphisher создает фальшивую точку доступа Wi-Fi и предоставляет ее пользователю вместо оригинальной;

— Infernal Twin также создает фальшивую точку доступа Wi-Fi; прогоаммное обеспечение используется для кражи паролей, фишинга, перехвата трафика;

— Aircrack-ng позволяет осуществлять перехват пакетов в беспроводной сети, их анализ и расшифровку; подходит для подключения к Wi-Fi с защитой в виде WEP или WPA шифрования;

— CommView for Wi-Fi — программное обеспечение для мониторинга и анализа данных в сетях стандартов 802.11 a/b/g/n/ac/ax; после захвата пакетов программное обеспечение отображает список точек доступа, узлов, уровни сигнала и другую информацию; программное обеспечение содержит модуль VoIP, который работает с голосовыми сообщениями SIP и H.323.

Перечисленные способы были ориентированы на персональный компьютер. Недостаток смартфона — его меньшая вычислительная мощность, которой может не хватить, например, для BruteForce, но взлом Wi-Fi возможен, например, https://tproger.ru/articles/6-hakerskih-programm-dlja-android-kak-ispolzujut-vash-wi-fi/).

Если чужой смартфон оказался у вас в руках (например, объект спит или отлучился), необходимо знать пароль для разблокировки экрана и, возможно, номер Apple ID:

1. Найдите диалог в списке чатов, «свайпните» по нему влево, выберите «Экспорт чата» и отправьте его, например, на свою почту. Это изменение, а также дата его совершения отобразится в Настройках.

2. Зайдите в WhatsApp в чат с самим собой, нажмите на «+» в левом нижнем углу, выберите «Местоположение» и «Делиться геоданными». Время, в течение которого будет доступна актуальная локация пользователя, можно настроить от 15 мин до 8 ч.

3. Всю информацию со смартфона можно скопировать: Настройки → Аккаунт → Изменить номер. Укажите другой номер. На него придет код подтверждения, а вся информация вместе с группами, медиафайлами и многим другим сохранится в приложении.

4. Благодаря функции резервного копирования, которая установлена по умолчанию, возможно удалить WhatsApp, переустановить его и увидеть архив чата с удаленными сообщениями.

5. Программное обеспечение VkurSe (https://vkur1.se/): запись аудио и видео; контроль переписки в социальных сетях и СМС; контроль местонахождения; удаленная блокировка смартфона; блокировка выбранных приложений; снятие скриншотов; автоматическая отправка данных на электронную почту.

6. При установке программного обеспечения: зарегистрируйтесь в выбранном сервисе и оплатите его использование; разрешите установку программного обеспечения из непроверенных источников; выполните настройки программного обеспечения; не трогайте настройки, назначение которых вам непонятно; не включайте ненужные функции, загружающие процессор и увеличивающие трафик; заранее создайте аккаунт для получения информации. После завершения установки почистите историю браузера и удалите установочный пакет.

Чтобы найти людей, находящихся поблизости, воспользуйтесь в Telegram функцией «Люди рядом», доступной только в мобильной версии: Перейдите в приложение Telegram → нажмите на три горизонтальные черточки в левом верхнем углу → перейдите в пункт «Люди рядом». Отобразятся контакты Telegram, находящиеся поблизости, а также все локальные чаты, которые были созданы в радиусе 6 км. Группы ранжируются по количеству участников в зависимости от удаленности от вас. Если контакт отобразится в списке, в чате

можно начать анонимное общение. Ваш номер телефона останется анонимным, пока вы не добавите человека в список своих контактов. По умолчанию данная функция отключена. Для того чтобы самому попасть в список «Люди рядом», нажмите на надпись «Показывать меня здесь». В вашем телефоне должна быть активна функция геолокации, а в настройках конфиденциальности приложения Telegram должно быть указано, что фотографии могут просматривать все контакты.

Есть несколько способов совершения звонков с подменой номера:

— для звонка через браузер понадобятся наушники с микрофоном; стоимость звонка — от 1 руб./мин.;

— для звонка через мобильный телефон нужно указать основной номер; стоимость звонка — от 3–4 руб./мин.;

— программное обеспечение SIP-System для защищенных звонков и СМС с подменой номера; администрация приложения не записывает логи звонков; стоимость одного аккаунта с подменой номера телефона — 690 руб.;

— сервис smska.us.

Методы ведения компьютерной разведки, методики и технологии ее проведения весьма близки к используемым в традиционной разведывательной деятельности. Применение компьютерной разведки обеспечивает:

— наблюдение за репутацией компании и формирование ее имиджа;

— отслеживание конкурентов, технологий или рынков сбыта;

— выявление возможных слияний и поглощений;

— оценку потенциальных рисков при инвестициях;

— выявление каналов утечки информации.

Мессенджер Telegram 12.03.2021 по требованию Роскомнадзора заблокировал бот «Глаз Бога» (@EyeOfGodOnionBot), который занимался поиском информации о людях, обращаясь к базам данных. Для поиска информации «Глаз Бога» использовал как открытые базы данных, так и базы данных, незаконно попавшие в Сеть. Его подписчиками являлось около 5 млн пользователей. Создатели сервиса называют его поисковой системой и заявляют, что для его использования

каждый пользователь обязан иметь согласие на обработку персональных данных от лица, чьи данные он собирается искать.

Сервисы ФМС МВД России:

— Проверка по списку недействительных российских паспортов: URL: http://services.fms.gov.ru/info-service.htm?sid=2000 http://xn--b1afk4ade4e.xn--b1ab2a0a.xn--b1aew.xn--p1ai/info-service.htm?sid=200;

— проверка недействительных заграничных паспортов старого образца сроком действия 5 лет: https://xn--b1agjhrfhd.xn--b1ab2a0a.xn--b1aew.xn--p1ai/services/invalidpass;

— проверка соответствия документа и адреса регистрации: http://xn--b1afk4ade4e.xn--b1ab2a0a.xn--b1aew.xn--p1ai/info-service.htm?sid=2160;

— проверка действительности разрешений на работу и патентов на осуществление трудовой деятельности иностранными гражданами и лицами без гражданства: http://xn--b1afk4ade4e.xn--b1ab2a0a.xn--b1aew.xn--p1ai/info-service.htm?sid=2060;

— проверка действительности приглашений на въезд в Российскую Федерацию иностранных граждан и лиц без гражданства: http://xn--b1afk4ade4e.xn--b1ab2a0a.xn--b1aew.xn--p1ai/info-service.htm?sid=2061;

— проверка наличия оснований для неразрешения въезда на территорию Российской Федерации иностранным гражданам и лицам без гражданства по линии МВД России: http://xn--b1afk4ade4e.xn--b1ab2a0a.xn--b1aew.xn--p1ai/info-service.htm?sid=3000.

Сервисы ФССП России:

— банк данных исполнительных производств: https://fssp.gov.ru/iss/ip/;

— розыск по исполнительным производствам, например, за неуплату алиментов: https://fssp.gov.ru/iss/suspect_info/ https://fssprus.ru/ iss/ip;

— проверка запрета на выезд из Российской Федерации: https://fssprus.net/proverit-zapret-na-vyezd-za-granitsu;

— проверка запрета на выезд из Российской Федерации по номеру исполнительного производства: https://pikabu.ru/story/.

Сервисы ФНС России:

— сервис ФНС России: https://service.nalog.ru/regmon/sign-in.html;

— проверка индивидуальных предпринимателей: https://pb.nalog.ru/;

— сервис определения ИНН физических лиц: https://service.nalog.ru/inn.do;

— выяснение, заблокированы ли банковские счета юридического лица или индивидуального предпринимателя: https://service.nalog.ru/bi.do;

— возможность узнать не только свою задолженность, но и других физических лиц, граждан Российской Федерации: https://service.nalog.ru/debt/;

— проверка организаций и индивидуальных предпринимателей на наличие компрометирующей информации: https://pb.nalog.ru/ index.html?&t=1607677244355;

— поиск финансовой отчетности российских компаний: https://bo.nalog.ru/;

— бесплатный сервис, который помогает узнать, зарегистрирован ли человек как плательщик налога на профессиональный доход (самозанятый): https://npd.nalog.ru/check-status/;

— получение выписки из ЕГРН об основных характеристиках и зарегистрированных правах на объект недвижимости (понадобится адрес, по которому проживает человек); предоставление сведений из ЕГРЮЛ/ЕГРИП в электронном виде: https://egrul.nalog.ru/index.html;

— проверка партнеров за 15–30 мин., включающая поиск по «черным спискам», определение фактического хозяина бизнеса, связи компании, ее учредителей, генерального директора с другими организациями; информация из ЕГРЮЛ): http://www.egrul-base.ru/ (цена 500 руб.);

— поиск сведений в реестре дисквалифицированных лиц: https://service.nalog.ru/disqualified.do;

— сервис определения задолженности по налогам: https://peney.net/.

— возможность убедиться в том, что паспорт принадлежит именно этому человеку — через сайт ФНС: https://service.nalog.ru/ static/personal-data.html?svc=inn&from=%2Finn.do — раздел «Узнать ИНН».

Сервис ФТС России:

— национальная часть единого реестра зарегистрированных таможенных деклараций, позволяющая определить кто, что, когда и откуда привез в нашу страну: http://188.254.71.82/rds_ts_pub/.

Сервисы судов России:

— по делам и судебным актам: https://sudrf.ru/index.php?id=300#sp;

— по текстам судебных решений: https://bsr.sudrf.ru/bigs/portal.html;

— сервис по судебным и нормативным актам, включающим решения судов общей юрисдикции, арбитражных судов и мировых судей с качественным удобным поисковиком: http://sudact.ru/;

— в банке решений арбитражных судов: https://ras.arbitr.ru/;

— в картотеке арбитражных дел: https://kad.arbitr.ru/;

— сервис для поиска и анализа судебной практики (позволяет анализировать судебную практику конкретного судьи): https://caselook.ru/#/search;

— единая база даных решений судов общей юрисдикции Российской Федерации: http://xn--90afdbaav0bd1afy6eub5d.xn--p1ai/;

— поисковик от «Яндекса» по судам общей юрисдикции (позволяет искать по номерам дел, ответчикам, истцам, отслеживать прохождение дел по всем инстанциям): http://www.gcourts.ru/;

— отдельно рекомендуется сайт Мосгорсуда: https://www.mosgorsud.ru/mgs/services/cases/first-criminal.

Сервисы нотариата:

— нотариальный портал (содержит список с координатами всех частных практикующих нотариусов России и нотариальных палат); для зарегистрированных пользователей доступна судебная практика нотариусов и файловый архив; база обновляется ежедневно (http://www.notary.ru/notary/bd.html);

— сервис проверки нотариальных документов: http://www.kartoteka.ru/ notariat/;

— возможность узнать, жив ли человек: https://notariat.ru/ru-ru/help/probate-cases/.

Сервисы ГИБДД МВД России:

— штрафы по государственному номеру автомобиля или номеру СТС: https://xn--90adear.xn--p1ai/check/fines;

— возможность проверить, действительно ли его водительское удостоверение и не лишали ли водительских прав: https://xn--90adear.xn--p1ai/check/driver#+;

— возможность проверить автомобиль по VIN-коду, номеру кузова или шасси: https://xn--90adear.xn--p1ai/check/auto гибдд.рф/check/auto/;

— проверка автомобиля по VIN-коду: https://avtocod.ru/;

— ресурс, где можно узнать историю автомобиля, зарегистрированного в Москве и Подмосковье, введя VIN-код и номер свидетельства о регистрации (выдача содержит: год выпуска, модель, цвет, мощность, экологический класс и объем двигателя, а также количество владельцев автомобиля, кроме того, выдаются данные о последнем пройденном техосмотре, о ДТП и возможных ограничениях): https://avtokod.mos.ru/;

— сервис проверки истории автомобиля по VIN-коду (история владения, история ДТП и аварий, кредитная история автомобиля): http://infovin.ru/.

Сервис Прокуратура Российской Федерации:

— Единый реестр проверок Генеральной прокуратуры Российской Федерации: https://proverki.gov.ru.

Другие государственные сервисы России:

— портал открытых данных Счетной палаты Российской Федерации: https://portal.audit.gov.ru/#/;

— реестр НКО, выполняющих функции иностранного агента: http://unro.minjust.ru/NKOForeignAgent.aspx.

Дополнительный поиск по физическим и юридическим лицам:

— находится ли имущество в залоге: https://www.reestr-zalogov.ru/search/index;

— реестр залогов движимого имущества: https://www.reestr-zalogov.ru/state/index;

— реестр уведомлений о залоге движимого имущества: https://www.reestr-zalogov.ru/#/;

— проверка документов об образовании: http://obrnadzor.gov.ru/ru/activity/main_directions/reestr_of_education/;

— сервис от Рособрнадзора по сведениям о документах об образовании и квалификации: http://obrnadzordov.ru/;

— сведения о банкротстве физических лиц: https://bankrot.fedresurs.ru/?attempt=;

— проверка реестра доверенностей: https://reestr-dover.ru/;

— проверка объектов недвижимости: https://www.росреестр-выписка.онлайн/;

— бесплатная проверка объекта недвижимости: https://rosreestr.gov.ru/wps/portal/online_request;

— справочная информация по объектам недвижимости в режиме онлайн от Федеральной службы государственной регистрации, кадастра и картографии: https://rosreestr.ru/wps/portal/cc_information_online; публичная кадастровая карта: https://pkk.rosreestr.ru/#/search/66.08075299999886,100.05436299999829/3/@6mmb5wv9;

— 101 база и реестр по бизнесу на Украине на одном ресурсе: https://protocol.ua/ua/101_publichniy_reestr_ukraini_polzuytes_1/;

— проверка компаний из Беларуси, России, Украины, Казахстана, Молдовы и Киргизии: https://legat.by/;

— сервис проверки партнеров в России: https://honestbusiness.ru/;

— проверка юридических и физических лиц: http://adnotamru.blogspot.com/ (на ресурсе богатейшая, хотя несколько беспорядочная коллекция полезнейших ссылок на сайты по проверке юридических и физических лиц; ссылки не только на российские ресурсы, но и на ресурсы Украины, Белоруссии, Казахстана);

— информация о предприятиях, находящихся в стадии банкротства (обобщается из «Коммерсанта», «Российской газеты»; информация с 2007 года по настоящее время); через расширенный поиск «Яндекса» отлично ищется по сайту: http://www.law-soft.ru/;

— бизнес-справки и проверка кредитных историй по любым компаниям и персоналиям по конкурентным ценам, а также многое другое: http://mbcredit.ru/;

— сервис проверки партнеров по официальным источникам статистики (наряду с получением данных по отдельной организации, позволяет в качестве дополнительной опции искать аффилированные

между собой организации, а также «пересечение» по генеральным директорам, собственникам и т. п.): https://focus.kontur.ru/;

— проверка партнеров: http://kontragenta.net/; https://zachestnyibiznes.ru/ http://datafabric.cc/tree;

— определение оператора по номеру или фрагменту номера телефона, месторасположение и т. п.: http://rossvyaz.ru/activity/num_resurs/registerNum/;

— Единый федеральный реестр сведений о банкротстве: http://bankrot.fedresurs.ru/;

— «Черный список» по российским строительным компаниям: http://www.stroi-baza.ru/forum/index.php?showforum=46;

— предоставление данных бухгалтерской отчетности по запросам пользователей: http://www.gks.ru/;

— сервис по проверке личности: http://dossier.scorista.ru/;

— обширная коллекция сервисов по проверке «всего и вся»: http://stop-list.info/;

— открытые данные компаний, товаров, услуг, сервисов, тендеров Российской Федерации: https://business-rating.company/;

— установление пользователя мобильного телефона и его примерного местоположения посредством агрегирования данных о номере из общедоступных источников (телефонных книжек, банковских сервисов, социальных сетей, объявлений, ЕГРЮЛ): телпоиск.ру;

— каталог организаций России (доступны полные данные по 12 млн организаций): http://www.list-org.com/;

— информация о юридических лицах и индивидуальных предпринимателях (поиск по названиям, адресу, руководителю, учредителю, ОГРН и ИНН): https://www.rusprofile.ru/;

— комплексный агрегатор официальной компрометирующей информации на физических лиц: https://datame.online/;

— сравнение финансового состояния фирмы с отраслевыми показателями и конкурентами: https://www.testfirm.ru/;

— история человека в Google: https://takeout.google.com/;

— поиск скрытых данных в социальной сети «ВКонтакте»: 220vk.com vk.city4me.com.

Дополнительные сервисы МВД России:

— список террористов и экстремистов: https://fedsfm.ru/ documents/terrorists-catalog-portal-act;

— федеральный список экстремистских материалов: https://data.gov.ru/opendata/7707211418-spisokekstremistov;

— возможность проверить, находится ли человек в розыске за совершение преступлений: https://xn--b1aew.xn--p1ai/wanted.

Сервис ФСИН России:

— розыск: https://fsin.gov.ru/criminal/.

Сервисы банков:

— проверка и восстановление банковских счетов: http://www.audit-it.ru/software/acmania.php;

— все, что нужно знать о долгах: http://dolgi.ru/servisy.

Другие сервисы по России:

— сервис раскрытия информации по эмитентам ценных бумаг Российской Федерации: http://www.e-disclosure.ru/;

— ОГРН: http://xn--c1aubj.xn--80asehdb/;

— наиболее полный ОГРН-каталог компаний России: https://ogrn.site/;

— сведения о договорах обязательного страхования: https://nsso.ru/check_policy/gop/contract/;

— постоянно пополняемая база деклараций о доходах и имуществе публичных должностных лиц: депутатов, чиновников, судей, представителей региональной и муниципальной власти, иных органов, госкорпораций и госкомпании: https://declarator.org/;

— проверка компаний в Российской Федерации: http://kartoteka.ru.

Сервисы по зарубежью:

— Интерпол: https://www.interpol.int/How-we-work/Notices/View-Red-Notices;

— «Их разыскивает Интерпол»: https://www.interpol.int/notice/search/wanted;

— ФБР: https://www.fbi.gov/wanted;

— исчерпывающая и структурированная база данных для проверки компаний на территории Республики Беларусь: http://alexandr-sel.livejournal.com/33499.html#cutid1;

— сервис для проверки партнеров на Украине http://fellix13.livejournal.com/6683.html;

— реестр задолженностей по исполнительным документам Республики Беларусь: https://minjust.gov.by/directions/enforcement/debtors/;

— сервис проверки партнеров по Беларуси: https://kartoteka.by/;

— платформа по списанию и продаже долгов в Беларуси: https://dolgovnet.by/;

— сервис проверки партнеров в Беларуси: https://contragento.by/;

— ЕГРЮЛ и частные предприниматели Беларуси: http://egr.gov.by/egrn/index.jsp?content=Find;

— поисковик по украинским реестрам: https://youcontrol.com.ua/;

— проверка юридических лиц на Украине: https://youcontrol.com.ua/ru/;

— проверка юридических и физических лиц на Украине: http://forum.razved.info/index.php?t=5885;

— база данных офшорных компаний (320 тыс.) (российские граждане часто обнаруживаются как их владельцы): https://offshoreleaks.icij.org/.

2.7. Примеры компьютерной разведки

Можно привести следующие примеры компьютерной разведки.

В 1999 г. в юридический отдел Американского бизнес-центра в г. Южно-Сахалинске поступило поручение руководства о проведении экспертизы готовящегося контракта. Сотрудник отдела готовит с использованием Интернета досье на контрагента, после чего дает заключение, что экспертизу проводить не нужно: за 10 мин. он обнаруживает компанию-контрагента в реестре должников и еще в каком-то черном списке.

Одна из разработанных технологий называется «следящий веб-каталог»: программное обеспечение автоматически собирает информацию по заданной теме (например, торговле оружием в Алжире)

с нескольких тысяч англоязычных источников новостей. Подборка новостей тут же переводится на русский язык.

В 2010 г. Фонд электронных рубежей выиграл иск к Министерству юстиции США и пяти другим федеральным ведомствам, в котором в соответствии с Законом о свободе информации требовал раскрыть секретные инструкции, описывающие работу спецслужб с социальными сетями. Полученный на руки в результате разбирательства 33-страничный документ свидетельствовал о том, что правительственные агенты используют сайты Facebook, MySpace, Linkedln, Twitter и другие социальные ресурсы, создавая фальшивые учетные записи.

Приложение Strava, кроме прочего, собирает данные со спортивных GPS-трекеров и отображает их на карте. Чем больше используется маршрут разными людьми, тем ярче он светится. Оказалось, что в некоторых регионах посреди пустыни на карте видны активные маршруты, ограниченные относительно небольшой площадью. Кроме того, в этих районах приложением Strava пользуются только военные США. Это позволяет утверждать, что там, где есть активность, располагается военная база. К примеру, это справедливо для Афганистана. Публичные данные, которыми поделился пользователь-военнослужащий, указывают не только на местоположение базы, но и на график смены патрулей, маршрутов их прохождения и другие детали, состав которых очевидно является военной тайной.

В российской армии приказы запрещают использование любых личных передающих устройств на территории военных объектов, что служит причиной постоянных жалоб со стороны военнослужащих, однако способствует сохранению военной тайны.

Исследователи из США отслеживали сигналы мобильных телефонов, находившихся на полигоне в Неноксе (Архангельская область) Было установлено 48 мобильных устройств, часть из которых позднее переместилась в Москву, Санкт-Петербург, Северодвинск и Архангельск. Одно из устройств переместилось в Азербайджан, а еще одно — на Кубу. Утверждается, что для слежки использовались данные GPS, которые фиксируют мобильные приложения потребителей.

Служба тыла Министерства обороны Израиля разместила на портале по чрезвычайным ситуациям карту расположения центров

тестирования на коронавирус по всей стране. Интерактивная карта позволяет вместе с гражданскими центрами локализовать секретные объекты израильской армии.

С помощью поисковых запросов, связанных с ядерным оружием, были обнаружены данные с шести американских военных баз. В 2013–2021 гг. военнослужащие США в Европе использовали приложения для заучивания информации. Карточки, помогающие в запоминании материала, попали в Интернет. Найдена информация о расположении камер, частоте патрулей, пароли и особенности пропусков.

В 2022 г. в сеть «утекли» база данных «Яндекса» и Delivery:

— https://saverudata.info/map/#lng=30.18704;lat=59.85851;zoom=19 (Работает только через VPN);

— https://saverudata.info/ и https://saverudata.info/map/.

Итак, в рамках данной главы было дано понятие об информационной потребности, а также рассмотрены возможности для ее удовлетворения доступными интернет-средствами. Приведены примеры добычи информации, которые могут оказаться полезными в деятельности МВД России.

Вопросы для самоконтроля:

1. В чем разница между данными и информацией?

2. Что такое потребность? На какие группы Эпикур разделил потребности человека? К какой из этих групп вы бы отнесли потребность в информации?

3. Дайте характеристику уровней отчетности при проведении компьютерной разведки.

4. Что составляет правовую основу проведения компьютерной разведки? Что является законодательной основой проведения гласной компьютерной разведки; негласной компьютерной разведки?

5. Перечислите основания для проведения компьютерной разведки в рамках оперативно-розыскной деятельности. В каких случаях допускается проведение компьютерной разведки без судебного решения?

6. Какие способы поиска информации в Интернете вы знаете? Какие типы поисковых сервисов вы знаете?

7. Как работает поисковая система? Что такое метапоисковая система?

8. Как осуществляется дополнительная фильтрация результатов выдачи?

9. Перечислите инструменты поиска информации о физических лицах в социальных сетях; в поисковых системах; по геолокации.

10. Как осуществить проверку доменного имени корпоративного сайта? Как получить сведения о компании из ЕГРЮЛ и ЕГРИП? Какие сервисы можно дополнительно использовать для поиска информации о компании?

11. Перечислите приемы аналитики, осуществляемой сотрудниками ФНС России, по результатам компьютерной разведки.

12. Перечислите сервисы федеральных органов исполнительной власти, используемые в компьютерной разведке.

ЗАКЛЮЧЕНИЕ

Обобщая изложенный в учебном пособии материал, напомним, что деятельность по добыче информации свойственная не только человеку и млекопитающим, но и птицам, и насекомым. Эта потребность сформировалась в процессе эволюции и с развитием технологий только нарастает. «Кто владеет информацией, тот владеет миром» — эти слова английского политического деятеля У. Черчилля можно считать началом современной информационной эпохи. Общие закономерности развития общества не обошли стороной и правоохранительные органы. С момента своего возникновения он были ориентированы на добычу оперативно-0розыскной информации, а в рамках информационного общества к этому добавилась необходимость получения оперативно-розыскной информации с помощью современных IT — компьютерной разведки.

К сожалению, специалистов в области получения компьютерной информации среди сотрудников органов внутренних дел мало, а программное обеспечение для проведения компьютерной разведки централизованно пока не поставляется, поэтому на сегодняшний день сотрудники органов внутренних дел, как правило, для проведения компьютерной разведки могут пользоваться только уже готовым программным обеспечением, наиболее эффективное из которого является платным.

СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

Нормативные правовые акты:

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

2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ.

3. Налоговый кодекс Российской Федерации от 31.07.1998 № 146-ФЗ.

4. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм., внесенным федеральным законом от 31.07.2020 № 278-ФЗ.

5. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности».

6. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

7. Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

8. Федеральный закон от 07.02.2011 № 3-ФЗ «О полиции».

9. Постановление Правительства Российской Федерации от 27.08.2005 № 538 (ред. от 17.04.2021) «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность».

10. Постановление Правительства Российской Федерации от 12.04.2018 № 445 «Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи».

11. Постановление Пленума Верховного Суда Российской Федерации от 24.12.1993 № 13 (ред. от 06.02.2007) «О некоторых вопросах, связанных с применением статей 23 и 25 Конституции Российской Федерации».

Основная литература:

1. Компьютерная разведка : учебное пособие / сост. Е. С. Поликарпов. — Краснодар : Краснодарский университет МВД России, 2018. — 198 с.

2. Поликарпов Е. С. Основы компьютерной разведки : учебное пособие. — Москва : Московский университет МВД России им. В. Я. Кикотя, 2020. — 321 с. // Национальная электронная библиотека. URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_BIBL_A_012606620/ (дата обращения: 24.03.2023).

Дополнительная литература:

1. Винокуров С. А. и др. Основы кибербезопасности : учебник. — Воронеж : Воронежский институт МВД России, 2022. — 503 с.

2. Воронов Ю.П. Компьютерная разведка : учебное пособие. — Новосибирск: НГУ, 2007. — 159 с.

3. Говоров А. Роль открытой информации и тенденции ее использования разведсообществом и министерством обороны США // Зарубежное военное обозрение. 2012. № 12. С. 26–31.

4. Додонов А. Г. и др. Конкурентная разведка в компьютерных сетях. — Киев : ИПРИ НАН Украины, 2013. — 250 с.

5. Зенин А. Разведка в сухопутных войсках США на основе анализа открытых источников информации // Зарубежное военное обозрение. 2009. № 5. С. 32–38.

6. Перминов Г. В. Практикум по компьютерной разведке в информационных сетях / Г. В. Перминов, С. П. Алексеенко, С. В. Родин. — Воронеж : Воронежский институт МВД России, 2014. — 147 с.

7. Ющук Е. Л. Интернет-разведка: руководство к действию. — Москва : Вершина, 2007. — 256 с.

8. Ющук Ю. Л. Сбор информации с «закрытых» форумов Невидимого Интернета. На примере экстремистских групп. Конспект-перевод статьи из New scientist // Сайт «Конкурентная разведка». URL: http://ci-razvedka.ru/Sbor-Informatsii-S-forumov-Nevidimogo-Interneta.html (дата обращения: 04.05.2022).

9. Якупов Р. А., Якупова Д. В. Прогнозы развития СССР в отражении аналитических материалов ЦРУ США (1981–1991) // Известия

высших учебных заведений. Поволжский регион. Гуманитарные науки. 2018. № 1 (45). С. 105–114.

Интернет-источники:

1. Open-source intelligence (OSINT) «ATP 2-22.9» // Информационный бюллетень OSINT № 33 (сентябрь — октябрь 2013 г.). URL: https://rykovodstvo.ru/exspl/19617/index.html (дата обращения: 17.01.2023).

2. Статистика поисковых систем. URL: https://drmax.su/statistika-poiskovyh-sistem-2020.html#stat-2-2 (дата обращения 24.09.2022).

3. Частые вопросы о Поиске Яндекса. URL: http://help.yandex.ru/search/ (дата обращения 24.09.2022).

Для заметок

Для заметок

Для заметок

Учебное издание

Якушев Денис Игоревич,
доктор технических наук;
Жидков Дмитрий Николаевич,
кандидат юридических наук

КОМПЬЮТЕРНАЯ РАЗВЕДКА

Учебное пособие

Редактор *Корчуганова И. А.*
Компьютерная верстка *Душкова А. Ю.*
Дизайн обложки *Шеряй А. Н.*

ISBN 978-5-91837-735-2

EDN UZBVIW

Подписано в печать 27.06.2023. Формат 60x84 $^{1}/_{16}$
Печать цифровая. Объем 5,5 п. л. Тираж 100 экз. Заказ № 45/23

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