РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

НИЖЕГОРОДСКАЯ АКАДЕМИЯ МВД РОССИИ

Министерство внутренних дел Российской Федерации
Нижегородская академия

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Допущено Министерством внутренних дел Российской Федерации в качестве учебного пособия для курсантов и слушателей образовательных организаций системы МВД России, сотрудников органов внутренних дел Российской Федерации

Нижний Новгород
НА МВД России
2023

УДК 373
ББК 67.408.1
Р24

Рецензенты:
кандидат юридических наук *О. Н. Игнатова*
(Следственный департамент МВД России);
кандидат юридических наук, доцент *Э. Д. Нугаева,*
кандидат технических наук *З. И. Харисова*
(Уфимский юридический институт МВД России);
доктор юридических наук, профессор *В. А. Мещеряков*
(Воронежский институт МВД России);
учебно-методическая секция по уголовно-правовым
и уголовно-процессуальным учебным дисциплинам (модулям)

Р24 **Расследование** преступлений в сфере компьютерной информации и иных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий : учебное пособие / Р. С. Поздышев, А. Е. Васильев, А. Г. Саакян, Т. А. Николаева, О. И. Долгачева. – Нижний Новгород : Нижегородская академия МВД России, 2023. – 77 с.

В учебном пособии содержатся системные сведения о преступлениях в сфере компьютерной информации и иных преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий, основанные на опыте расследования уголовных дел за 2019–2023 гг. Представлена квалификация и типология преступлений в сфере компьютерной информации и предложены меры по решению проблемных вопросов по совершенствованию правоприменительной практики в данной сфере, а также раскрыты криминалистические и процессуальные особенности производства следственных и иных процессуальных действий в ходе расследования преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

Пособие дополняет учебный материал дисциплин «Расследование преступлений в сфере компьютерной информации», «Уголовное право», а также «Криминалистика» по темам, связанным с особенностями квалификации и расследования преступлений, совершаемых с использованием информационных технологий.

Издание предназначено для курсантов и слушателей образовательных организаций Министерства внутренних дел Российской Федерации, обучающихся по специальности «Правовое обеспечение национальной безопасности» (специализация – уголовно-правовая) и может быть использовано в практической деятельности сотрудниками органов предварительного следствия, а также в рамках их служебной подготовки.

ISBN 978-5-88840-196-5

Печатается по решению редакционно-издательского совета
Нижегородской академии МВД России

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Трансформационные процессы, связанные с цифровизацией жизни, несут не только позитивные изменения, но и характеризуются рядом угроз общественной безопасности, поскольку криминальные элементы незамедлительно имплементируют все современные разработки в преступные схемы. Количество преступлений, совершаемых в Российской Федерации (далее – РФ) с использованием информационно-телекоммуникационных технологий, ежегодно возрастает, а их способы становятся все более изощренными. В 2017 г. их число увеличилось на 37,4 % (90 587); рост в 2018 г. – на 92,8 % (174 674); 2019 г. – на 68,5 % (294 409); 2020 г. – на 73,4 % (510 396); 2021 г. – на 1,4 % (517 722); 2022 г. – на 0,8 % (522 065)[1].

Работа по противодействию этим преступлениям не в полной мере соответствует необходимому уровню и вызывает озабоченность первых лиц государства. На данный факт в ходе расширенного заседания коллегии МВД России обратил внимание Президент РФ В. В. Путин[2].

Преступления в сфере компьютерной информации среди всех криминальных деяний, совершаемых с использованием информационно-телекоммуникационных технологий, представляют собой наиболее характерную их разновидность. В настоящее время они, хотя и имеют незначительный удельный вес в общей структуре преступности в данной сфере, однако проявляют стойкую тенденцию к ежегодному росту. На их базе возможно рассмотреть криминалистически важные технические и организационные аспекты информационно-телекоммуникационных технологий, проанализировать существующую юридическую практику в данной сфере, а также разработать рекомендации по производству следственных и иных процессуальных действий по уголовным делам указанной категории.

Данные результаты исследования с определенной адаптацией к конкретным следственным ситуациям достаточно эффективно могут быть применены и при расследовании иных преступлений, совершение которых не связано с использованием информационно-телекоммуникационных технологий. Например, данные знания могут быть полезны при установлении места нахождения скрывшегося подозреваемого или обвиняемого. Таким образом, несмотря на то, что непосредственным предметом настоящего исследования в первую очередь явились преступления в сфере компьютерной информации, круг читателей учебного пособия не ограничивается сотрудниками органов внутренних дел, специализирующимися на раскрытии и расследовании данных преступлений, и обучающимися по соответствующим учебным дисциплинам.

Компьютеризация криминального мира является серьезным вызовом правоохранительной системе, которая выступает в роли догоняющего.

---

[1] Состояние преступности. URL: https:// мвд.рф/reports (дата обращения: 10.03.2023).

[2] Расширенное заседание коллегии МВД России 17.02.2022. URL: http://www.kremlin.ru/events/president/news/67795 (дата обращения: 10.03.2023).

Действительный уровень подготовки сотрудников органов внутренних дел в данной сфере остается недостаточным для эффективного противодействия киберпреступности. Значительная часть правоприменителей плохо осведомлена о способах использования информационно-телекоммуникационных технологий в криминальных целях, а те, кто обладает такими знаниями, считают, что современные способы анонимизации в сети не позволяют установить личность преступника.

В правоприменительных актах нередко встречается ошибочное использование терминологии, связанной с компьютерными технологиями, что свидетельствует об искаженном представлении данных понятий в сознании многих сотрудников. Это обстоятельство, в свою очередь, не только не способствует раскрытию преступлений, но и формирует в криминальной среде устойчивое мнение о низком уровне профессиональной подготовки правоохранительных органов в данной сфере, дополнительно мотивируя на совершение подобных деяний. Представляется, что данное учебное пособие позволит сделать очередной шаг в направлении решения указанной проблемы.

Эмпирическая база учебного пособия представлена материалами судебно-следственной практики (обвинительные заключения, постановления о прекращении уголовных дел, приговоры и др.) по противодействию преступлениям в сфере компьютерной информации, которые предоставлены Следственным департаментом МВД России в 2022 г. в рамках подготовки заказного научного исследования «Аналитический обзор результатов работы органов предварительного следствия по уголовным делам о преступлениях в сфере компьютерной информации по итогам 2021 года», а также результатами интервьюирования 48 сотрудников органов внутренних дел, проходящих службу в разных регионах РФ, в чьи обязанности входит противодействие преступлениям в сфере компьютерной информации.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМАЯ ИНФОРМАЦИЯ ОБ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЯХ

Интернет (англ. *INTERconnected NETworks* – «соединенные сети») – Всемирная компьютерная сеть, множество узлов которой составляют взаимодействующие по единым правилам компьютеры и компьютерные устройства, работающие в составе независимых пакетных сетей с различными архитектурами, техническими характеристиками и территориальным размещением[1].

Иными словами, интернет – объединение всех локальных компьютерных сетей. На базе этой объединенной сети работают интернет-сервисы (электронная почта, Всемирная паутина, сервисы мгновенного обмена сообщениями, интернет-телефония и др.), позволяющие взаимодействовать и обмениваться информацией между электронными устройствами, в том числе компьютерами, по всему миру.

Понятие и виды IP-адресов

При взаимодействии каждое электронное устройство представляется узлом сети, который принимает и передает информацию от других компьютерных устройств, также являющихся узлами сети. Для того чтобы один узел мог обратиться к другому, им присваиваются IP-адреса. Кроме того, каждое устройство, способное подключаться к компьютерной сети, имеет mac-адрес. Отличие данных адресов заключается в следующем: mac-адрес присваивается производителем сетевого устройства, обычно указан на самом устройстве и по умолчанию остается неизменным на протяжении всего жизненного цикла устройства; IP-адрес присваивается интернет-провайдером[2] узлу, через который компьютерное устройство подключается к интернету, данный адрес не постоянно привязан к устройству и может изменяться при смене интернет-провайдера или при каждом новом выходе в сеть.

Для более детального понимания IP-адреса следует рассмотреть данное понятие, проведя его классификацию.

По формату выделяются следующие разновидности IP-адресов:

1) IPv4 – состоят из комбинации четырех чисел от 0 до 255, каждое из которых разделяется точкой (например, 95.127.255.0). Таким образом, возможны около 4,22 млрд вариаций адресов;

2) IPv6 – состоят из комбинации восьми чисел, записанных в шестнадцатеричной системе счислений (то есть цифрами от 0 до 9 и буквами латинского алфавита от A до F): например, fa23:12da:34cb:1234:cd09:ac87:4321:af56.

---

[1] Большая российская энциклопедия. URL: https://bigenc.ru/technology_and_technique/text/2014701 (дата обращения: 15.09.2023).

[2] *Интернет-провайдер* – организация, представляющая услуги доступа к сети «Интернет». Одними из наиболее крупных и популярных в России являются ПАО «Ростелеком», «МТС», «Мегафон», «Вымпелком» и др.

Данные адреса пришли на смену IPv4 в связи с ростом количества компьютерных устройств, способных подключаться к сети (кроме компьютеров, изначально формировавших интернет, сейчас подключаются к сети и соответственно получают свой уникальный IP-адрес смартфоны, умные часы, смарт-телевизоры, бытовая техника с функцией «умный дом» и др.).

В настоящее время существуют IP-адреса обоих форматов.

По виду компьютерной сети IP-адреса подразделяются на:

1) частные (внутренние, локальные, приватные, «серые») – используются в локальных компьютерных сетях для взаимодействия локальных устройств между собой без прямого подключения к интернету. В сети «Интернет» данные адреса не используются. Для них выделены следующие диапазоны: 10.0.0.0–10.255.255.255; 100.64.0.0–100.127.255.255; 172.16.0.0–172.31.255.255; 192.168.0.0–192.168.255.255. Данные адреса должны быть уникальны в пределах своей локальной сети и могут подключаться к другой сети (интернету) через маршрутизатор (роутер). Такие адреса используются, например, в компьютерной сети предприятия или домашней сети, когда к маршрутизатору (в том числе посредством Wi-Fi-соединения) подключаются компьютерные устройства;

2) публичные (внешние, глобальные, «белые») – предназначены для использования в сети «Интернет»; являются уникальными в рамках глобальной сети (рис. 1).

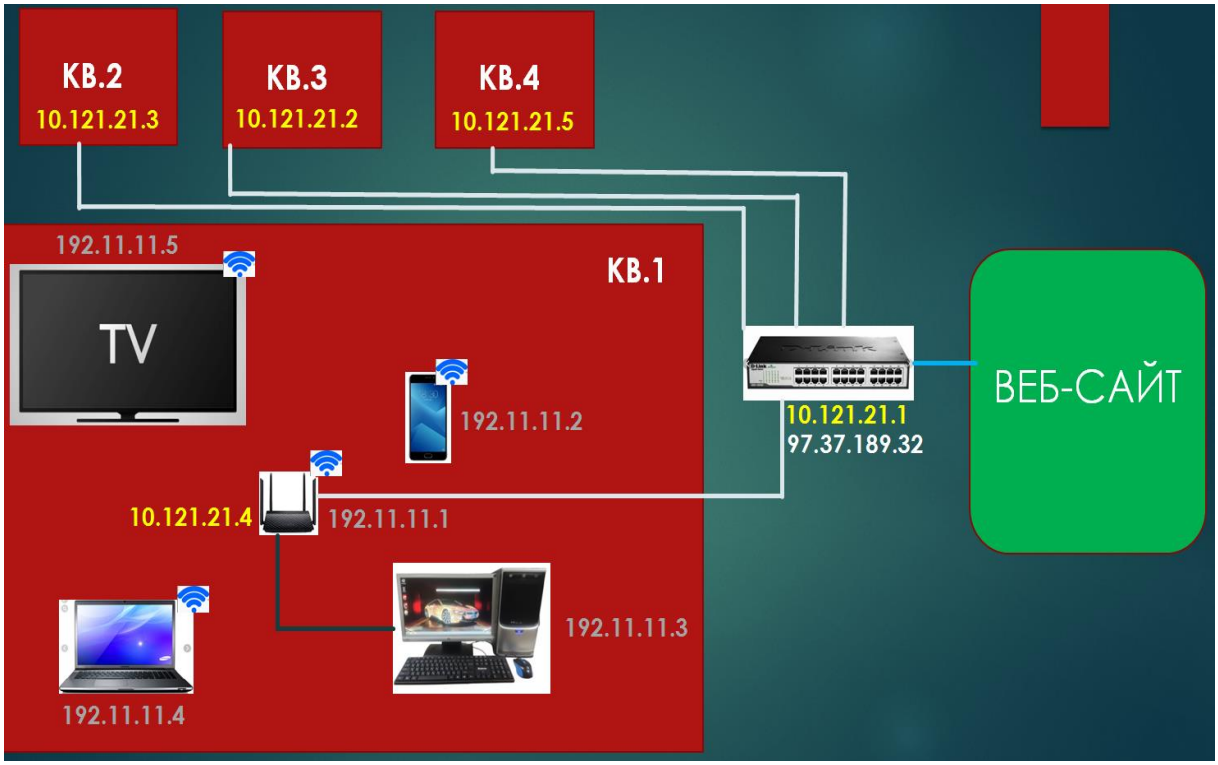

Рис. 1. *Локальная сеть и интернет. Частные и публичные IP-адреса (IP-адреса 192.* – локальная сеть квартиры; IP-адреса 10.* – локальная сеть подъезда дома; IP-адрес 97.37.189.32 – публичный, присвоен коммутатору в подъезде дома, его видят веб-сайты, таким образом все пользователи в данном подъезде выходят в сеть «Интернет» под одним публичным IP-адресом)*

Криминалистическое значение данной классификации IP-адресов заключается в том, что веб-сайт может предоставить информацию только в отношении IP-адреса, присвоенного коммутатору интернет-провайдера, являющемуся шлюзом для выхода в сеть «Интернет» определенного количества клиентского оборудования, например, расположенного в одном подъезде многоквартирного дома. Интернет-провайдер в свою очередь, получив от правоохранительных органов точное время предоставления IP-адреса и сетевой адрес интернет-ресурса, к которому происходило подключение, может предоставить информацию в отношении клиента, с которым заключен договор оказания услуг доступа к сети «Интернет». В случае домашнего интернета будут предоставлены установочные данные лица, с которым заключен договор, и адрес оказания услуг. В случае мобильного интернета будут предоставлены установочные данные лица и его абонентский номер.

По стабильности при переподключениях к сети IP-адреса подразделяются на:

1) статические – выдаются интернет-провайдером в постоянное пользование клиенту, то есть за все время использования услуг по доступу в интернет у пользователя будет один и тот же IP-адрес, независимо от переподключений к сети (даже если клиент не подключен к интернету, провайдер не может передать в пользование другим лицам его IP-адрес). Статический IP-адрес необходим для обеспечения удаленного доступа к определенному устройству (узлу сети) и встречается редко, поскольку в условиях своего ограниченного диапазона у интернет-провайдера целесообразнее представлять обычным клиентам их динамическую разновидность;

2) динамические – также выдаются интернет-провайдером, но не по принципу «один адрес – один клиент», а распределяются между всеми пользователями по необходимости, то есть при каждом подключении к сети клиенту выдается случайный IP-адрес из пула адресов, закрепленных за данным провайдером, который после отключения одного пользователя передается другому, желающему воспользоваться услугами доступа к интернету. Возникновение динамических адресов явилось решением проблемы ограниченного количества IP-адресов в условиях непрерывно растущего числа пользователей.

Исходя из результатов интервьюирования сотрудников органов внутренних дел, в чьи должностные обязанности входит противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, правоприменителями нередко ошибочно трактуется понятие динамического IP-адреса: связывают его с невозможностью или значительным затруднением в установлении личности пользователя, использующего данный тип интернет-адресации. В действительности данное обстоятельство не является препятствием для деанонимизации пользователя, поскольку интернет-провайдер владеет полной информацией о том, какой IP-адрес и в какое время был предоставлен определенному клиенту.

Соответственно, в таком случае в запросе кроме самого IP-адреса необходимо указывать точное время (до секунды) выхода в сеть.

Значительные трудности в правоприменительной среде вызывают случаи, когда интернет-провайдер предоставляет один IP-адрес одновременно нескольким клиентам (до сотен и тысяч одновременно). Этот механизм распределения адресов называется NAT (от англ. *Network Address Translation* – «преобразование сетевых адресов»). Он призван решить проблему ограниченного количества IP-адресов. Механизм стал широко распространенным, когда сформировалось убеждение в том, что даже при использовании динамической адресации число пользователей превышает возможности сети. Иными словами, интернет-провайдеры создают множество локальных сетей для своих клиентов, где распределяют между ними частные IP-адреса, и в тех случаях, когда всем этим клиентам необходим выход в интернет, провайдер направляет их через один внешний IP-адрес.

Таким образом, серверы, к которым обращаются все указанные пользователи (например, веб-сайты), видят один и тот же IP-адрес и отправляют запрашиваемую клиентом информацию на него. Этот адрес, в свою очередь, распределяет полученные данные по исходным адресатам. Наибольшее распространение такая система сетевой адресации получила у операторов сотовой связи при оказании услуг мобильного интернета.

В связи с изложенным, очевидно, что интернет-провайдеру известно, какой конкретно пользователь обращался к определенному ресурсу, несмотря на то, что под данным внешним IP-адресом одновременно выходило в сеть «Интернет» множество его клиентов. Для эффективной выборки и деанонимизации пользователей в таком случае необходима не только информация об IP-адресе и времени его использования (как в случае с динамической адресацией), но и сведения об адресе интернет-ресурса, к которому делал запрос пользователь.

Всемирная паутина (Веб)

Под Всемирной паутиной (англ. *World Wide Web*, сокр. – *WWW*, *Web*) понимается распределенная неоднородная компьютерная система коллективного пользования гипермедийными документами, действующая на базе сети «Интернет»[1]. Ключевым элементом Всемирной паутины является веб-сайт (от англ. *web-site*: *web* – «паутина, сеть» и *site* – «место», буквально – «место, сегмент, часть в сети») – веб-страница или несколько связанных между собой веб-страниц, которые воспринимаются пользователем как единое целое и хранятся на веб-сервере (компьютере со специальным программным обеспечением).

В соответствии с Федеральным законом от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[2] под

[1] Большая российская энциклопедия. URL: https://bigenc.ru/technology_and_technique/text/3923747 (дата обращения: 15.09.2023).

[2] Собрание законодательства РФ. 2006. № 31, ч. 1, ст. 3448.

веб-сайтом понимается совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет».

Для просмотра веб-сайтов используются веб-браузеры (от англ. *web-browser*: *web* – «паутина, сеть» и *browser* – «обозреватель», буквально – «обозреватель сети») – компьютерная программа, позволяющая находить и просматривать документы, размещенные в интернете. Наиболее популярными на сегодняшний день являются Google Chrome, Яндекс Браузер, Mozilla Firefox и др.

Каждый сервер веб-сайта – узел компьютерной сети, наряду со смартфонами, маршрутизаторами (роутерами), компьютерами и др. Как и всякий узел сети, сервер веб-сайта имеет свой IP-адрес, который является статическим, поскольку если бы он постоянно изменялся, у пользователей не было бы возможности обращаться к нему стабильно.

Адреса сайтов по своему виду не отличаются от других IP-адресов и также представлены числами. Однако для удобства запоминания адресов веб-сайтов используются доменные имена, состоящие из символов, разделенных между собой точкой (точками): мвд.рф; yandex.ru, где каждый набор символов между точками представляет домен определенного уровня (рис. 2).

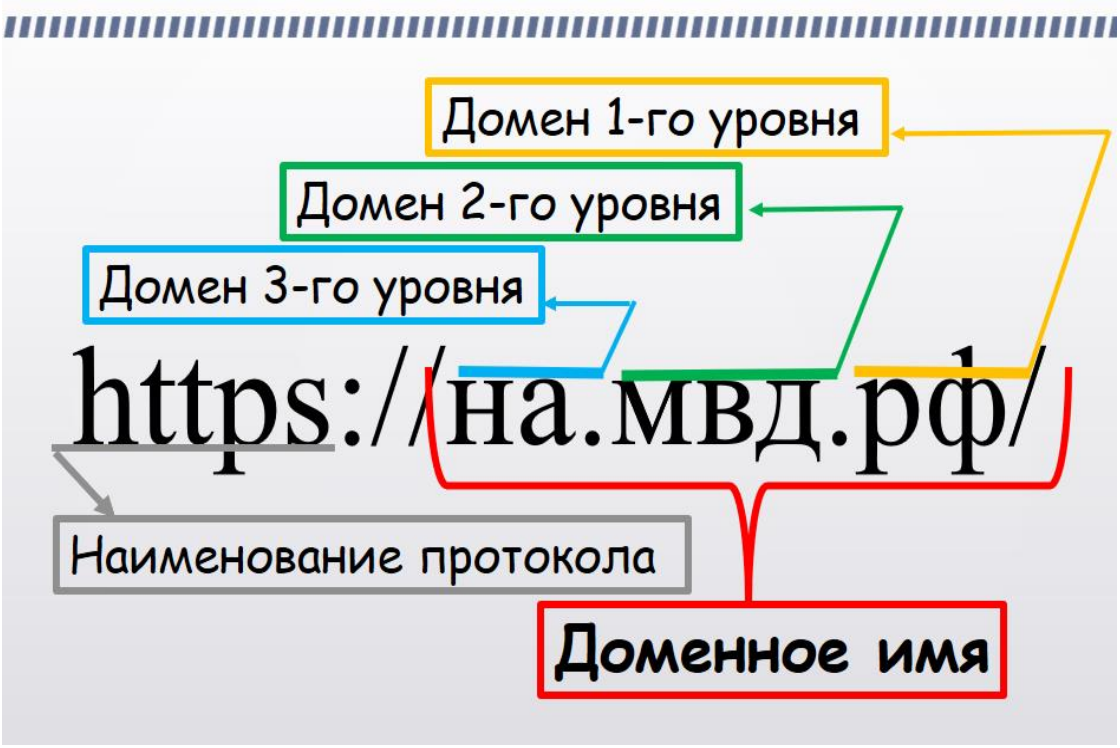

Рис. 2. *Доменное имя*

Первичными в сети являются IP-адреса, и все устройства обращаются друг к другу по ним, поэтому после введенного в веб-браузере доменного имени веб-сайта он должен найти его IP-адрес в DNS (англ. *Domain Name*

System – «система доменных имен») – реестре данных, где указаны доменные имена и соответствующие им IP-адреса путем обращения к DNS-серверу (рис. 3).

Рис. 3. *Упрощенная схема взаимодействия персонального компьютера пользователя с DNS-сервером и веб-сайтом*

Даркнет

Под даркнетом (от англ. *darknet*: *dark* – «темный», *net* – «сеть», также дарквеб, «темная сеть», «скрытая сеть», «темный веб») понимается теневой сегмент Всемирной паутины, соединения которой устанавливаются только между доверенными устройствами с использованием нестандартных протоколов и портов[1].

Для четкого понимания данного явления необходимо указать на его соотношение со смежными понятиями. Итак, существует Всемирная паутина, в которой можно выделить три сегмента.

Первый – это «поверхностный веб», клирнет (от англ. *Clear Net* – «чистая сеть»; сурфейс веб (от англ. *Surface Web* – «поверхностная сеть»), составляющий по различным оценкам от 3 до 5 % от общего объема данных, размещенных в вебе. Здесь находится общедоступная информация, которую любой пользователь может найти с помощью поисковых систем.

Второй сегмент – «глубокий веб» (от англ. *Deep Web* – «глубокая сеть»), доля которого равна примерно 90 %. В нем содержится информация, которая также находится в открытой части Всемирной паутины, но не индексируется поисковыми системами, доступ к ней имеют только автори-

[1] Что такое даркнет и почему там продаются наши данные: РБК-тренды. URL: https://trends.rbc.ru/trends/industry/602f668a9a7947d5f06e0c7a#:~:text=Даркнет%20 (дата обращения: 15.09.2023).

зованные пользователи. К такой информации относятся, например, письма электронной почты, различные базы данных коммерческих и государственных структур и др.

Третий сегмент – даркнет, объем которого составляет примерно 6 % от общего размера информации, размещенной в сети. Он находится в так называемой закрытой части интернета, доступ к которой невозможен с использованием обычного браузера – необходимо специальное программное обеспечение.

Даркнет в значительной степени связан с некоммерческой организацией Tor Project, Inc., целями которой являются обеспечение доступа к интернету без цензуры для каждого и обеспечение максимальной приватности и свободы в сети. Говоря о целях и мотивах данной организации, авторский коллектив опирается на публичные заявления ее представителей, размещенные на официальном сайте юридического лица[1].

Наименование Tor (далее – Тор) является аббревиатурой от англ. *The Onion Routing*[2], дословно означающей «луковая маршрутизация».

Как отмечалось ранее, интернет-трафик (информация, передаваемая в сети) по умолчанию идет от одного узла сети (клиента) к другому узлу (серверу) в виде запроса определенной информации (например, веб-сайта) и затем обратно от сервера к клиенту в виде ответа (например, содержимое веб-сайта). Идея «луковой маршрутизации» начала разрабатываться в 1990-е гг. в США и заключалась в недопущении прямых обращений клиента к серверу путем перенаправления трафика через цепочку узлов сети, при этом шифруя его на каждом этапе (по аналогии со слоями луковицы).

Сеть «Тор» начала работать в октябре 2002 г. Ее код был опубликован с бесплатной и открытой лицензией. Таким образом, данная сеть является программным обеспечением с открытым исходным кодом, который доступен любому лицу для просмотра, изучения и изменения. Эта особенность предоставляет каждому пользователю возможность убедиться в отсутствии уязвимостей и неприемлемых для пользователя функций (например, скрытого слежения), принять участие в доработке данной открытой программы, использовать код для создания новых программ и исправления в них ошибок.

В 2008 г. для более широкого распространения и простого использования сети «Тор» был разработан Tor Browser (далее – Тор-браузер) – программа с открытым исходным кодом, обеспечивающая доступ к сети «Тор».

Существуют и иные программы-браузеры, а также расширения для обычных браузеров, позволяющие подключение к данной сети, но Тор-браузер разработан непосредственно организацией Tor Project, Inc. В настоящее время существуют версии Тор-браузера для компьютеров с наиболее

---

[1] Tor Project, Inc. URL: https://www.torproject.org (дата обращения: 15.09.2023).

[2] Даркнет представлен не только сетью «Тор», но и иными сетями со специфическими протоколами доступа, скрытыми от обычных пользователей сети «Интернет». Так, в теневом сегменте сети существует сеть I2P, также известная как сеть с «чесночной маршрутизацией». В настоящем учебном пособии рассматривается только сеть «Тор», поскольку она имеет наибольшую популярность в криминальной среде.

популярными операционными системами: Windows, Linux и macOS. Есть версия для смартфонов на базе Android. Кроме того, популярным приложением, с помощью которого весь трафик Android-устройства проходит через сеть «Tor», является Orbot. Официальной версии Tor для смартфонов на базе IOS нет, однако существует множество приложений, позволяющих направлять трафик Apple-смартфона через сеть «Tor» (например, Onion Browser).

Указанные программные продукты, включая Tor-браузер, позволяют обращаться не только к ресурсам даркнета, но и к обычным веб-сайтам, при этом в любом случае маршрутизируют трафик через сеть «Tor».

Все интернет-ресурсы сети «Tor» расположены в домене «.onion» (от англ. *onion* – «лук»), например, http://xmh57jrzrnw6insl.onion, и, в отличие от доменных имен открытой части интернета, в своем наименовании имеют множество случайных символов, присваиваемых автоматически.

Рассмотрим работу сети «Tor» (см. рис. 4).

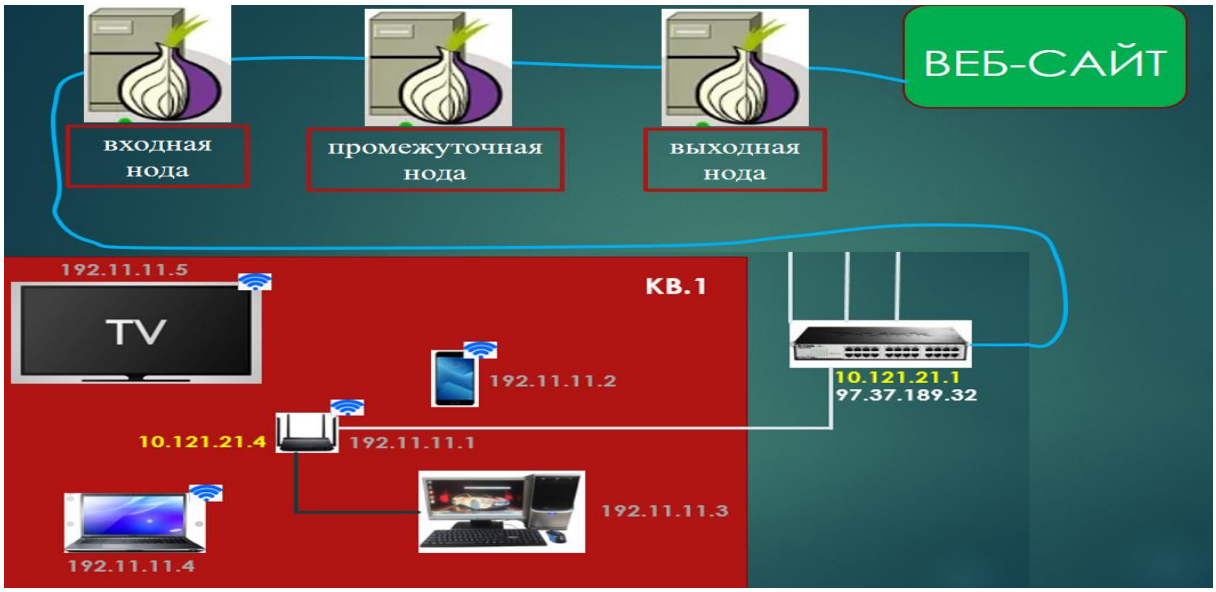

Рис. 4. *Упрощенная схема работы сети «Tor»*

Нода – это узел сети «Tor», через который проходит трафик. Любой запрос клиента к серверу осуществляется через три узла сети «Tor» – три ноды: входную, промежуточную и выходную. При этом информация как поступающая от клиента, так и возвращающаяся ему с сервера, шифруется на каждом этапе по протоколу HTTPS.

Таким образом, каждая нода получает информацию в зашифрованном виде, то есть не знает ее содержания, при этом обладает сведениями только об IP-адресе предыдущего и последующего узлов, но не знает одновременно IP-адреса клиента и сервера. Сервер (например, веб-сайт), к которому обращается пользователь, видит лишь IP-адрес выходной ноды и не знает IP-адрес клиента. Описанные обстоятельства серьезно усложняют процесс установления личности пользователя сети «Tor», и его действия зачастую выглядят как работа пользователя из другого государства (местонахождения выходной ноды).

Интернет-провайдер также не обладает информацией о том, к какому интернет-ресурсу обращается его клиент; он видит только факт входа клиента в Tor (база ноды сети «Tor» находится в открытом доступе). Информация, которую клиент получает из сети, также не известна, поскольку поступает в зашифрованном виде.

В качестве ноды выступают другие пользователи, определенным образом настроившие свои компьютерные устройства для данной цели (не любой пользователь). Таким образом, каждый пользователь сети «Tor» решает самостоятельно, предоставлять свой компьютер для работы в качестве ноды или нет. При настройках по умолчанию данная функция не реализуется[1].

Поисковой системой Tor-браузера по умолчанию является DuckDuckGo, обеспечивающая высокий уровень анонимности, по сравнению с наиболее популярными поисковыми системами (например, Google, Yandex и др.).

Однако DuckDuckGo осуществляет поиск так же, как и другие распространенные поисковые системы, только в «поверхностном вебе». В даркнете есть свои поисковые системы, которые индексируют веб-сайты лишь в данном сегменте Всемирной паутины (например, Torch, NotEvil и др.). В даркнете размещается значительное количество веб-сайтов различной тематики, в число которых входят и те, что в открытой форме предлагают противоправные услуги и товары, в том числе наркотические средства, поддельные документы и денежные купюры.

Одним из наиболее популярных в русскоязычном даркнете до недавнего времени являлся сайт «Гидра» (Hydra, http://hydraruzxpnew4af.onion), прекративший в апреле 2022 г. работу в связи с задержанием его администраторов[2]. В настоящее время популярными криминальными сайтами даркнета считаются BlackSprut, OMG, Mega и др.

Все они являются торговыми площадками, на которых взаимодействуют продавцы и покупатели различных незаконных товаров и услуг. Интерфейс и принципы работы аналогичны торговым площадкам в обычном интернете. Здесь представлены различные магазины, товары, форумы и отзывы, руководства для покупателей и продавцов.

Для регистрации пользователя достаточно придумать логин и пароль; указания дополнительной информации в виде электронной почты или номера телефона, как правило, не требуется. Любой пользователь может зарегистрировать свой магазин и осуществлять сбыт незаконных товаров

---

[1] В представленном учебном пособии особенности работы сети «Tor» и смежных программных продуктов рассматриваются максимально упрощенно. Более подробную информацию и ответы на интересующие вопросы можно найти на сайте https://www.torproject.org в разделах «Поддержка», «Сообщество», «Блог».

[2] *Снегов Е.* Миф о русской «Гидре». Чем закончилась история крупнейшей площадки по продаже наркотиков (и кончилась ли). URL: https://secretmag.ru/criminal/mif-o-russkoi-gidre-chem-zakonchilas-istoriya-krupneishei-ploshadki-po-prodazhe-narkotikov-i-konchilas-li.htm (дата обращения: 15.09.2023).

на данной торговой площадке, где осуществляется общение между покупателем и продавцом, каждому из которых известны только условное имя (никнейм) другого.

Оплата товара обычно реализуется в криптовалюте «биткоин», что также способствует высокому уровню анонимности взаимоотношений преступников. Передача товара осуществляется бесконтактным способом: через оставление в тайнике либо через службы доставки с использованием подложных установочных документов. Визуальные примеры информации, размещенной на данных криминальных маркетплейсах, приведены в приложении 1.

Иные популярные средства анонимизации пользователя в сети «Интернет»

В настоящее время широкое распространение не только среди продвинутых пользователей компьютерной техники, но и простых обывателей получили прокси-серверы (англ. *proxy* – «представитель») и VPN-серверы (англ. *Virtual Private Network* – «виртуальная частная сеть»). Для целей учебного пособия принципы работы прокси и VPN существенных отличий не имеют. Эти средства представляют собой дополнительный узел в компьютерной сети, через который идет подключение к внешним сетевым ресурсам (например, веб-сайтам)[1].

Основное отличие между ними заключается в том, что через прокси-сервер перенаправляется только трафик, а VPN-сервер обеспечивает более высокий уровень безопасности, так как шифрует все данные, передаваемые между компьютером пользователя и сервером.

Таким образом, интернет-провайдер фиксирует трафик своего клиента только до VPN или прокси-сервера, а интернет-ресурс, к которому обращается клиент, не видит настоящий IP-адрес пользователя, а взаимодействует только с подменным IP-адресом (см. рис. 5).

Таким образом, у правоохранительных органов возникает проблема установления абонентского устройства пользователя таких средств анонимизации, поскольку ни интернет-провайдер, ни администратор веб-сайта не обладают полной информацией, необходимой для решения данной задачи, однако использование подобных средств анонимизации, так же как и сети «Тор», не является непреодолимым препятствием. Способы установления личности в таких следственных ситуациях будут раскрыты в третьей главе учебного пособия.

[1] VPN или прокси-сервер: что лучше и в чем разница? URL: https://www.kaspersky.ru/resource-center/preemptive-safety/vpn-vs-proxy-server (дата обращения: 21.03.2023).

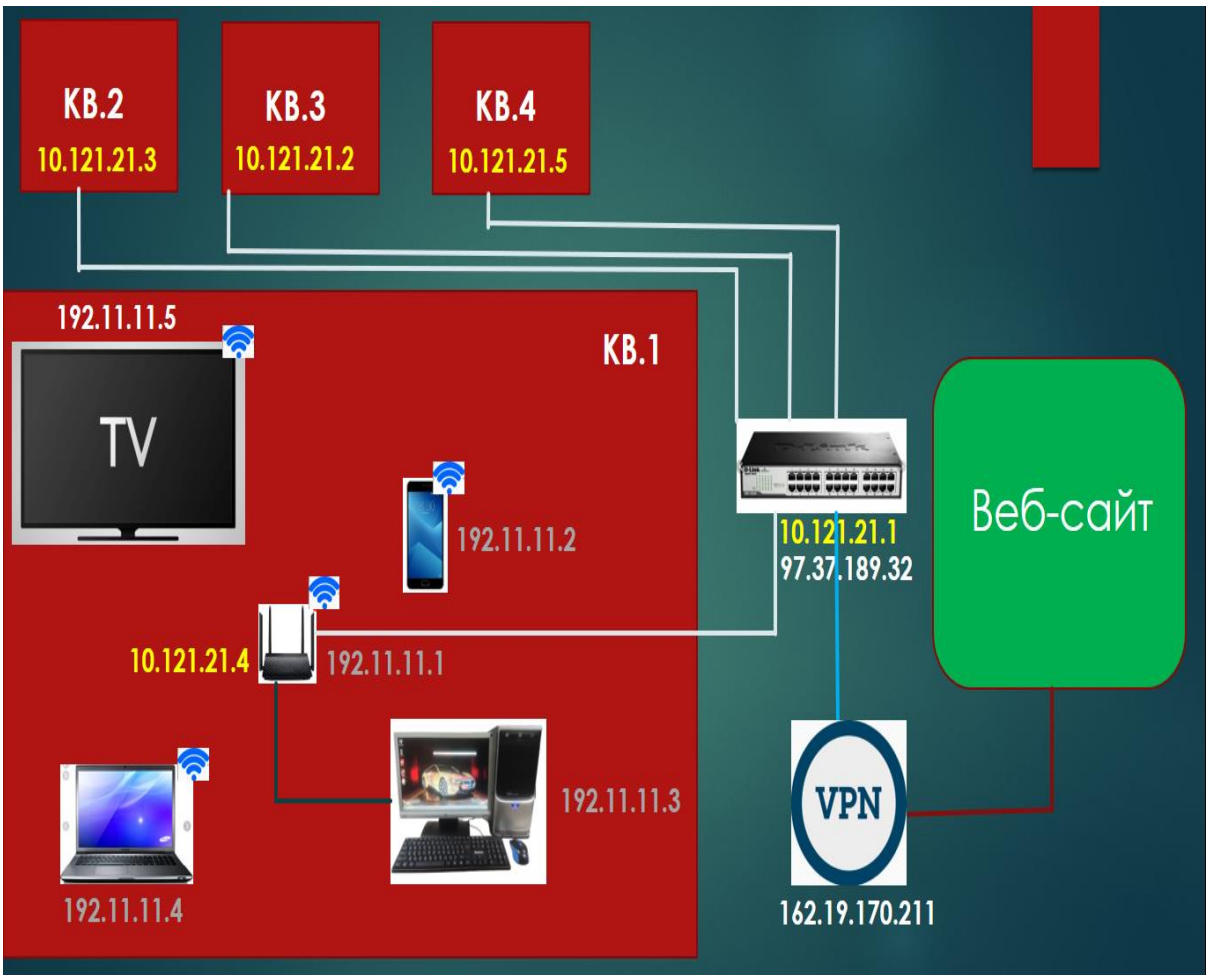

Рис. 5. *Схема подключения к интернет-ресурсу через VPN-сервер. Схема подключения идентична схеме, изображенной на рис. 1, за исключением того, что обращение к веб-сайту происходит не напрямую с коммутатора интернет-провайдера (внешний IP-адрес 97.37.189.32), а через VPN-сервер (IP-адрес 162.19.170.211)*

Сотовая связь и IP-телефония

Сотовая связь является разновидностью радиосвязи. Ключевыми звеньями сотовой сети выступают абонентские устройства (сотовые телефоны), приемопередающие базовые станции и коммутаторы. Базовые станции представляют собой вышки, на которых установлено специальное оборудование для приема и передачи сигнала сотовых телефонов, представляющее собой несколько разнонаправленных антенн, каждая из которых обслуживает свой сектор. Коммутаторы обеспечивают передачу сигнала между разными сегментами сетей, передавая и принимая сигналы в рамках одного оператора связи на уровне местных и междугородних сетей, а также передавая и принимая сигналы от сетей других операторов связи (см. рис. 6).

В развитии сотовой связи существует пять поколений. Сотовые сети поколения 1G (англ. *generation* – «поколение») получили распространение в 1980-е гг. Они были предназначены только для телефонных звонков в рамках сети одного оператора и передавали аналоговые сигналы.

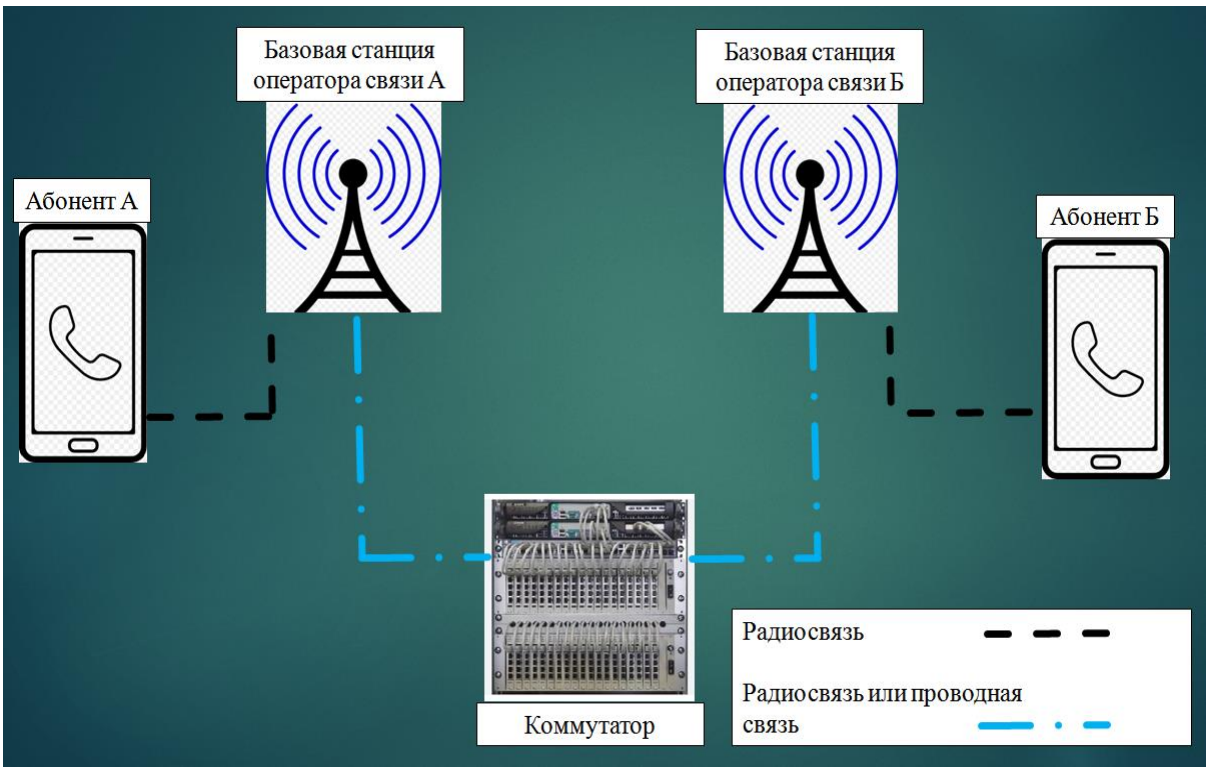

Рис. 6. *Упрощенная схема работы сотовой связи*

Поколение 2G (GSM) появилось в 1990-е гг., с использованием данных сетей сигналы передавались в цифровом формате и позволяли совершать не только телефонные звонки и отправлять короткие текстовые сообщения (SMS), но и передавать данные. Появился мобильный интернет, передача данных осуществлялась в формате GPRS, а впоследствии в формате Edge.

Дальнейшее развитие сотовой связи связано со спросом абонентов на более скоростной мобильный интернет. Так, в 2000-х гг. появляется поколение 3G, где высокоскоростная пакетная передача данных была реализована форматом мобильного интернета HSPA, в 2010-х гг.– поколение 4G форматом мобильного интернета LTE, а в настоящее время развивается пятое поколение сотовых сетей.

Как было описано выше, приемопередающие базовые станции оборудованы разнонаправленными антеннами. Понимание этого обстоятельства имеет криминалистически важное значение. Для установления местоположения абонентского устройства целесообразно устанавливать не только сведения об адресе приемопередающей базовой станции, но и сведения о количестве антенн и азимуте действия конкретной антенны, обслуживающей абонентское устройство.

Развитие сотовой связи, мобильного интернета, наличие возможностей передавать через сотовую сеть пакеты данных и кодировать (декодировать) эту информацию в различные форматы позволило использовать для цифровой передачи голоса IP-телефонию, то есть телефонную связь по протоколу IP.

Данная технология, как и многие другие информационные технологии, получила распространение не только в законных видах деятельности, но и была взята на вооружение преступным миром. Основную ценность такой технологии для криминальных элементов представляет возможность осуществлять звонки на любые телефоны с использованием сети «Интернет», скрывая настоящий абонентский номер лица, осуществляющего вызов.

Компьютер, выступающий в качестве сервера (виртуальной IP-телефонной станцией), позволяет при инициировании исходящего соединения указывать в пакетах данных любой абонентский номер, который прописывается в реквизите Caller ID (идентификатор вызывающего абонента).

Таким образом, на абонентском устройстве лица, получающего телефонный вызов, отражается подменный абонентский номер. Также эта не соответствующая действительности информация отображается в биллинге оператора связи данного лица. Схема работы IP-телефонии изображена на рисунке 7.

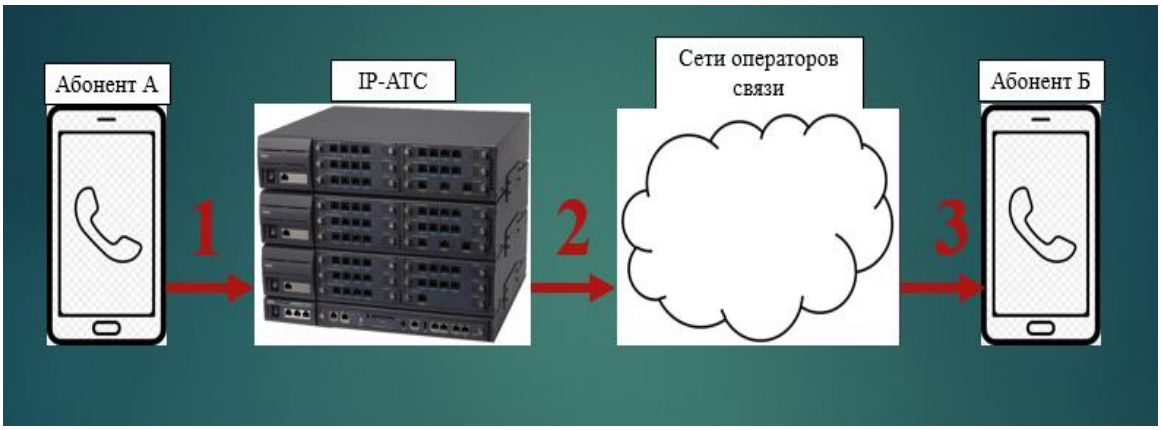

Рис. 7. *Упрощенная схема работы IP-телефонии.*
Шаг 1 – абонент А осуществляет подключение к серверу, выступающему виртуальной IP-АТС, используя свой настоящий абонентский номер.
Шаг 2 – сигнал абонента А преобразуется виртуальной IP-АТС и в качестве Caller ID прописывается иной абонентский номер, после чего сигнал с подменным абонентским номером передается в сети других операторов связи по маршруту к абоненту Б. Операторы данных сетей видят только подменный абонентский номер.
Шаг 3 – сигнал поступает на абонентское устройство абонента Б с отображением подменного номера

В настоящей главе кроме вышерассмотренных принципов работы IP-телефонии целесообразно рассмотреть актуальные законодательно закрепленные инструменты противодействия подмене абонентского номера.

Подмена абонентского номера законодательно запрещена Федеральным законом от 05.12.2017 № 386-ФЗ «О внесении изменений в статью 46 Федерального закона «О связи» и статью 1 Федерального закона «О внесении изменений в Федеральный закон «О связи»[1].

[1] Собрание законодательства РФ. 2017. № 50, ч. III, ст. 7557.

Данным нормативным правовым актом введен п. 9 ст. 46 Федерального закона от 07.07.2003 № 126-ФЗ «О связи»[1] (далее – ФЗ «О связи»), согласно которому оператор связи, в сети которого инициируется или устанавливается телефонное соединение, обеспечивается передача короткого текстового сообщения или инициируется соединение для целей передачи голосового сообщения, обязан передавать в сеть связи другого оператора связи в неизменном виде абонентский номер или уникальный код идентификации вызывающего абонента.

Однако в данном законе не было предусмотрено внесение изменений, устанавливающих юридическую ответственность оператора связи в случае неисполнения данной обязанности, а также не было установлено механизма проверки подлинности абонентского номера или уникального кода идентификации абонента.

Таким образом, цель исключить факты подмены абонентского номера, обозначенная субъектом законодательной инициативы[2], достигнута не была, а внесенные изменения обрели лишь декларативный характер.

Следующим этапом борьбы с подменными номерами стал Федеральный закон от 02.07.2021 № 319-ФЗ «О внесении изменений в Федеральный закон “О связи”»[3]. Данный нормативный правовой акт призван решить проблему отсутствия у оператора связи возможности проверить подлинность абонентского номера путем создания системы обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования. Порядок использования данной системы закреплен в постановлении Правительства РФ от 03.11.2022 № 1979 «Об утверждении Правил направления в систему обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования и получения из указанной системы сведений»[4].

Принцип работы данной системы заключается в следующем. Каждый оператор связи, действующий на территории России, должен быть подключен к системе и осуществлять с ней взаимодействие в автоматическом режиме. Оператор связи при инициировании установления соединения абонентом, завершении его установления или транзите трафика обязан передавать в данную систему соответствующие сведения, в том числе об абонентских номерах вызывающего и вызываемого абонента. Система, в свою очередь, имея доступ к этой информации, получаемой от всех российских операторов связи, проверяет, действительно ли указанный абонент определенного оператора совершает соответствующий вызов. Если система устанавливает отсутствие информации о реальном инициировании со-

---

[1] Собрание законодательства РФ. 2003. № 28, ст. 2895.

[2] Пояснительная записка к проекту федерального закона «О внесении изменений в статью 46 Федерального закона «О связи». URL: https://sozd.duma.gov.ru/bill/1030321-6 (дата обращения: 30.03.2023).

[3] Собрание законодательства РФ. 2021. № 27, ч. I, ст. 5147.

[4] Там же. 2022. № 46, ст. 7996.

единения абонентом, то становится понятным, что вызов осуществляется посредством IP-телефонии с использованием подменного абонентского номера. Данную информацию в течение 500 миллисекунд система передает оператору связи, в сети которого находится вызываемый абонент, а этот оператор должен в течение 2 секунд завершить данное соединение.

Для понимания эффективности работы системы обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования необходимо сделать два замечания.

Во-первых, для надлежащего функционирования данной системы к ней должны быть подключены все операторы связи, осуществляющие свою деятельность на территории России. Данный процесс требует финансовых и временных затрат, поэтому в настоящее время еще не завершился. По официальной информации, затраты операторов связи субсидируются государством, а переходный период, ведущий к полномасштабному функционированию системы, запланирован до 31 декабря 2024 г.[1] До этого момента операторы связи, не подключенные к системе, могут использоваться злоумышленниками как для подменных абонентских номеров, находящихся в их номерной емкости, так и для совершения преступлений в отношении их абонентов.

Во-вторых, данная система способна исключить подмену абонентских номеров только российских операторов связи, установить факт подмены иностранного абонентского номера с использованием такого инструментария невозможно.

Безусловно, на особое ослабление бдительности потерпевших влияет использование преступниками официальных абонентских номеров кредитных учреждений и правоохранительных органов в качестве подменных, однако очевидно, что найдутся люди, у которых не вызовет особых подозрений и иностранный абонентский номер. Кроме того, в настоящее время злоумышленниками уже используются иностранные телефонные коды вместо российского +7, но при этом напоминающие отечественные абонентские номера. Например, может использоваться префикс абонентского номера +8495, который схож с префиксом Московского региона (+7495), но в действительности относится к вьетнамским операторам связи.

Дальнейшим шагом борьбы с подменными номерами стало дополнение Кодекса РФ об административных правонарушениях ст. 13.2.1, введенной в действие Федеральным законом от 30.12.2021 № 480-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»[2]. Данная норма предусматривает административную ответственность за следующие правонарушения:

---

[1] Государство будет субсидировать создание системы обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика. URL: https://мсп.рф/services/news/digest/detail/gosudarstvo-budet-subsidirovat-sozdanie-sistemy-obespecheniya-soblyudeniya-operatorami-svyazi-trebov/ (дата обращения: 30.03.2023).

[2] Собрание законодательства РФ. 2022. № 1, ч. I, ст. 49.

– неисполнение оператором связи обязанности по передаче в неизменном виде абонентского номера и (или) уникального кода идентификации;

– неисполнение оператором связи обязанности по прекращению оказания услуг связи и (или) услуг по пропуску трафика в свою сеть связи в случае использования подменного абонентского номера;

– неисполнение оператором связи обязанности по подключению к системе обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования либо обязанности по направлению в систему обеспечения соблюдения операторами связи требований при оказании услуг связи и услуг по пропуску трафика в сети связи общего пользования и (или) по получению из указанной системы сведений.

Вопросы для самоконтроля

1. Дайте определение и проведите классификацию IP-адресов.
2. Что представляет собой система доменных имен?
3. Что представляет собой даркнет и какие принципы работы сети «Tor»?
4. Какие средства анонимизации личности в сети «Интернет» в настоящее время наиболее распространены? Объясните принципы их работы.
5. Каким образом преступники используют подменные абонентские номера и какие способы противодействия этому явлению существуют?

ГЛАВА 2. ПРОБЛЕМНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ И ТИПОЛОГИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Преступления в сфере компьютерной информации закреплены в гл. 28 Уголовного кодекса РФ (далее – УК РФ) и представлены в виде пяти статей (ст. 272–274^2), предусматривающих ответственность: за неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей; неправомерное воздействие на критическую информационную инфраструктуру РФ; нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

Для обзорных целей настоящей главы учебного пособия круг данных преступлений расширен: в него включено мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ), поскольку способ его совершения имеет общие признаки с рассматриваемой категорией криминальных деяний.

Проведенный анализ показал, что за 2019–2023 гг. максимальное распространение в большинстве регионов России получили преступления, связанные с неправомерным доступом к компьютерной информации. Мошенничество в сфере компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, а также неправомерное воздействие на критическую информационную инфраструктуру РФ занимают второе, третье и четвертое места соответственно.

Уголовные дела о преступлениях, предусмотренных ст. 274 и 274^2 УК РФ, в производстве следователей органов внутренних дел за указанный период не находились.

Неправомерный доступ к компьютерной информации

Фактические обстоятельства совершения деяний, подпадающих под действие ст. 272 УК РФ, неоднородны. Можно выделить два вида:

– условно неправомерный;

– безусловно неправомерный доступ к компьютерной информации.

Первый совершается лицами с использованием служебного положения. Доступ к компьютерной информации представляется им для профессиональной деятельности, но они используют свои полномочия вопреки установленным правилам обращения к такой информации.

Второй вид включает в себя преступления, совершаемые лицами, которые при любых обстоятельствах не имели права доступа к подобным сведениям.

Условно неправомерный доступ к компьютерной информации

Типичными преступлениями данного вида являются криминальные деяния, совершаемые работниками кредитных организаций и операторов сотовой связи.

В производстве Следственной части Главного следственного управления Главного управления Министерства внутренних дел России (далее – СЧ ГСУ ГУ МВД России) по Новосибирской области находилось уголовное дело по обвинению Л. в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ. Расследованием установлено, что в 2020 г. сотрудник ПАО «Вымпел Коммуникации» Л., используя свое служебное положение, не имея в распоряжении соответствующих заявлений клиентов, под своим служебным логином и паролем неоднократно неправомерно осуществлял доступ к охраняемой законом компьютерной информации, а именно: подыскивал в базе данных компании абонентские номера статуса «золотой» или «платиновый», которые на протяжении длительного периода не использовались их владельцами, после чего переоформлял их на свое имя, тем самым осуществляя блокирование и модификацию компьютерной информации. Доволенским районным судом Новосибирской области Л. осужден к лишению свободы условно, сроком на 1 год и 6 месяцев[1].

Аналогичные преступные деяния не всегда квалифицируются по ст. 272 УК РФ. В отечественной юридической практике есть примеры привлечения к уголовной ответственности за неправомерный доступ к компьютерной информации, содержащейся в базах данных операторов связи, по ст. 274[1] УК РФ. Подробнее об этом далее в настоящей главе.

Выделяющимся из общей массы криминальных деяний данного вида представляется преступление, совершенное сотрудником организации, основным видом деятельности которой является разработка компьютерного программного обеспечения.

В производстве СЧ ГСУ ГУ МВД России по г. Москве находилось уголовное дело, возбужденное по ч. 3 ст. 272 УК РФ. Установлено, что Ю., являясь системным администратором ООО «Я.Т.», осуществил неправомерный доступ и копирование идентификатора пользователя одного из почтовых ящиков специализированного сервиса компании, номера его мобильного телефона, ответа на контрольный вопрос, кода для криптографической подписи и порядкового номера ключа, которые посредством мессенджера «Джабер» передал неустановленному лицу. Люблинским районным судом г. Москвы Ю. признан виновным, ему назначен штраф в размере 300 000 рублей[2].

---

[1] Приговор Доволенского районного суда Новосибирской области от 11.10.2021 № 1-130/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

[2] Приговор Люблинского районного суда г. Москвы от 09.11.2021 № 01-0750/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

В условиях распространения коронавирусной инфекции возникли новые преступления, в том числе в сфере компьютерной информации.

СЧ СУ УМВД России по Астраханской области расследовано уголовное дело в отношении медсестры У., которая, используя ставшие ей известными в ходе осуществления трудовой деятельности логин и пароль на имя медицинской сестры К., осуществила неправомерный доступ к Федеральному регистру вакцинированных от COVID-19, куда внесла недостоверную информацию об иммунизации лиц с использованием вакцин для профилактики COVID-19. Красноярским районным судом Астраханской области по уголовному делу в отношении У. вынесен обвинительный приговор с назначением наказания в виде штрафа в размере 20 000 рублей[1].

В настоящее время практика привлечения к уголовной ответственности за неправомерный доступ к Федеральному регистру вакцинированных от COVID-19 характеризуется неоднозначностью, подобные деяния, совершенные при схожих обстоятельствах, квалифицируются как по ст. 272 УК РФ, так и по ст. 274[1] УК РФ. Подробнее об этом далее в настоящей главе.

Безусловно неправомерный доступ к компьютерной информации

Преступления данного вида имеют более неоднородный состав и характеризуются разным уровнем общественной опасности. Одними из наиболее характерных здесь являются деяния, связанные со взломом учетных записей на различных интернет-ресурсах, например, в социальных сетях и маркетплейсах.

В производстве СЧ СУ УМВД России по Оренбургской области находилось уголовное дело по обвинению Н. в совершении 21 преступления, предусмотренного ч. 2 ст. 272 УК РФ. В ходе предварительного следствия установлено, что Н. путем подбора и ввода данных – логина и пароля, которые заблаговременно приобрел на специализированном сайте, не имея на то разрешения обладателя информации, осуществил неправомерный доступ к учетным записям граждан в социальной сети «ВКонтакте», после чего изменил пароли к данным профилям, заблокировав к ним доступ для законных пользователей. В дальнейшем Н. использовал учетные записи для совершения мошеннических действий. Приговором Промышленного районного суда г. Оренбурга Н. осужден к 2 годам лишения свободы с отбыванием наказания в колонии-поселении[2].

Растущая угроза кибербезопасности в виде неправомерного доступа к компьютерной информации, ее шифрование и последующее требование о выкупе ключей для расшифровки является общемировым трендом. Россия

---

[1] Приговор Красноярского районного суда Астраханской области от 21.12.2021 № 1-196/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

[2] Приговор Промышленного районного суда г. Оренбурга от 17.03.2021 № 1-10/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

не является исключением. В производстве нескольких территориальных органов МВД России в 2019–2023 гг. находились уголовные дела о подобных преступлениях, по ряду из которых удалось установить лиц, подлежащих привлечению в качестве обвиняемого, и успешно завершить расследование.

В производстве ГСУ ГУ МВД России по Алтайскому краю находилось уголовное дело по обвинению П. в совершении двух преступлений, предусмотренных ч. 2 ст. 272 УК РФ. Расследованием установлено, что П. приобрел на неустановленных интернет-ресурсах информацию, необходимую для удаленного доступа к персональным компьютерам бухгалтеров организаций в Челябинской области и Краснодарском крае. Используя эти сведения (IP-адрес, логин, пароль), П. осуществил неправомерный доступ к данным бухгалтерии, заархивировал их, удалив оригинальные файлы, и установил пароли для доступа к архивам. За предоставление паролей доступа к заблокированной информации П. получил от представителей организаций выкуп в криптовалюте DASH. Приговором Армавирского городского суда Краснодарского края П. назначено наказание в виде исправительных работ на срок 1 год 2 месяца с удержанием 10 % заработной платы в доход государства[1].

Следующей группой преступлений рассматриваемого вида неправомерного доступа к компьютерной информации являются деяния, связанные с деятельностью фишинговых сайтов.

СЧ ГСУ ГУ МВД России по Саратовской области в суд направлено уголовное дело по обвинению М. в совершении ряда преступлений, предусмотренных ч. 2 ст. 272 УК РФ, а именно в том, что он, используя средства разработки, создал и зарегистрировал в ООО «Регистратор доменных имен РЕГ.РУ» фишинговые веб-сайты, имеющие внешнее визуальное сходство с интернет-ресурсом ПАО «Ростелеком». При этом в указанные сайты был встроен алгоритм, позволяющий копировать охраняемую законом компьютерную информацию, составляющую банковскую тайну (значения полей, обозначенных как «Номер банковской карты», «Срок действия банковской карты (ММ/ГГ), «Код CVV/CVC», «Имя держателя банковской карты»). В дальнейшем производилась отправка указанной информации на адреса электронной почты М. для ее последующего использования в корыстных целях[2].

Три вышеуказанных типа преступлений представляют наибольшую общественную опасность по сравнению с иными криминальными деяниями, подпадающими под признаки выделяемого нами вида неправомерного доступа к компьютерной информации. Это обусловлено необходимым для преступника высоким уровнем владения специальными знаниями в сфере

---

[1] Приговор Армавирского городского суда Краснодарского края от 28.09.2021 № 1-469/2021 // Интернет-ресурс Судебные и нормативные акты РФ (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

[2] Приговор Октябрьского районного суда г. Саратова от 15.03.2022 № 1-330/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

информационных технологий и, как из этого следует, более существенным ущербом, наносимом обществу. Следует заметить, что значительную долю в практике следователей органов внутренних дел составляют менее серьезные преступления, связанные с неправомерным доступом к компьютерной информации. Данные преступления, в отличие от вышеназванных, могут не восприниматься гражданами как уголовно наказуемые, в связи с чем нередко совершаются не в полной мере осознанно. К таким деяниям относятся факты неправомерного доступа к развлекательному контенту.

СУ УМВД России по г. Белгороду расследовано уголовное дело по ч. 2 ст. 272 УК РФ в отношении К., который в период 2019–2021 гг., используя ресиверы с модифицированными смарт-картами «Триколор ТВ», осуществлял просмотр спутниковых телеканалов, тем самым несанкционированно принимал (копировал) компьютерную информацию в виде закодированных ECM-сообщений и CW-кодовых слов, содержащихся в системе спутникового телевидения, в результате чего НАО «Национальная спутниковая компания» причинен материальный ущерб на сумму 26 141 рубль 70 копеек. Приговором Октябрьского районного суда г. Белгорода К. осужден к штрафу в размере 20 000 рублей[1].

С цифровизацией образовательного процесса распространение получили преступления, связанные с неправомерным внесением изменений в электронные журналы учебных занятий.

В производстве СУ УМВД России по Тамбовской области находилось уголовное дело по обвинению А. в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ.

Установлено, что последний, являясь отчисленным студентом ТОГАПОУ «Колледж техники и технологии наземного транспорта им. М. С. Солнцева», используя логин и пароль от учетной записи преподавателя К. в системе «Дневник.ру», осуществил неправомерный доступ к электронному журналу, содержащему охраняемую законом компьютерную информацию, и изменил оценки некоторым студентам колледжа, а также от имени указанного преподавателя оставил комментарии оскорбительного содержания студентам и преподавателю Т. В последующем с целью блокирования доступа преподавателя К. к его учетной записи А. изменил пароль доступа к регистрационной учетной записи, необходимой для использования личного кабинета преподавателя. Знаменским районным судом Тамбовской области уголовное дело в отношении А. в соответствии со ст. 94 УК РФ прекращено по п. 3 ч. 1 ст. 24 УПК РФ (в связи с истечением сроков давности уголовного преследования)[2].

---

[1] Приговор Октябрьского районного суда г. Белгорода от 12.08.2021 № 1-334/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

[2] Постановление Знаменского районного суда Тамбовской области от 26.03.2021 № 1-21/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

Дистанционные виды хищений нередко связаны с неправомерным доступом к компьютерной информации, так как данное деяние в ряде случаев является способом обеспечения доступа к чужому имуществу.

Типичным примером является уголовное дело (СЧ СУ УМВД России по Архангельской области) по обвинению Д. в совершении нескольких преступлений, в том числе одного, предусмотренного ч. 2 ст. 272 УК РФ.

Доказано, что обвиняемая с целью тайного хищения денежных средств подыскала на сайте «Авито» объявление о продаже куртки за 3 000 рублей, размещенное В. Далее Д., выдавая себя за покупателя, якобы для перевода денежных средств в качестве предоплаты, получила от потерпевшей реквизиты ее банковской карты. После чего, используя мобильное приложение «ВТБ Онлайн» и код, переданный потерпевшей, произвела вход в личный кабинет последней и изменила абонентский номер, на который приходили уведомления от банка, тем самым модифицировав и заблокировав компьютерную информацию. 31 января 2022 г. уголовное дело направлено в суд для рассмотрения по существу.

Создание, использование и распространение вредоносных компьютерных программ

Преступления, предусмотренные ст. 273 УК РФ, которые в 2019–2023 гг. расследовались органами предварительного следствия в системе МВД России, можно разделить по признаку уровня специальных знаний, которыми обладают преступники: профессиональное создание, использование и распространение вредоносных компьютерных программ и непрофессиональное использование и распространение таких продуктов.

Профессиональное создание, использование и распространение вредоносных компьютерных программ

Данные преступления характеризуются высоким уровнем квалификации в сфере компьютерных технологий. Нередко преступники имеют высшее образование в данной сфере и существенный опыт в программировании и смежных профессиях. Это обусловливает серьезное противодействие раскрытию и расследованию подобных преступлений, выражающееся в тщательной конспирации при подготовке и совершении криминальных деяний.

В производстве СУ УМВД России по Пензенской области находилось уголовное дело по обвинению К., З. и А. в совершении преступления, предусмотренного ч. 2 ст. 273 УК РФ. В начале 2019 г. обвиняемые, проживающие в разных субъектах РФ, через сеть «Интернет» договорились о создании вредоносной программы, предназначенной для получения несанкционированного доступа к компьютерной информации, и последующем ее распространении за денежное вознаграждение для использования иными лицами. При этом К. занимался разработкой и написанием программного

кода, корректировкой приложения и его модернизацией. Задачами двух других обвиняемых было тестирование вредоносной программы, поиск потенциальных клиентов, их консультирование и продажа программы заинтересованным лицам.

Злоумышленники соблюдали строгие меры конспирации: общение происходило через анонимные мессенджеры, учетные записи и электронные почтовые ящики; на постоянной основе использовалось программное обеспечение для подмены IP-адресов; регулярно менялись сетевые идентификаторы, виртуальные номера сотовой связи.

Созданное обвиняемыми приложение оставалось незамеченным всеми антивирусными программами, позволяло без ведома пользователей через любой доступный канал (ссылки в социальных сетях, прямую рассылку во вложениях к электронным письмам, добавление к программному коду легитимной программы, скачиваемой пользователем и т. д.) заражать их компьютеры, незаконно копировать информацию о логинах и паролях для доступа к различным интернет-сервисам, а также сведения о банковских картах, используемых для электронных платежей.

Полученные данные применялись неустановленными лицами для хищения денежных средств с банковских счетов лиц, находившихся в США, Канаде и странах Евросоюза. Ленинским районным судом г. Пензы обвиняемые осуждены к различным срокам лишения свободы[1].

Отдельно среди данного вида преступлений следует выделить атаки типа «отказ в обслуживании» (DDoS-атаки, от англ. *DDoS – Distributed Denial of Service*). Особую активность такая преступная деятельность получила в 2022 г. в отношении российских коммерческих организаций, а также органов государственной и муниципальной власти.

СЧ ГСУ ГУ МВД России по г. Санкт-Петербургу и Ленинградской области расследовано уголовное дело, возбужденное по ч. 2 ст. 273 УК РФ. В ходе предварительного следствия установлено, что в 2018–2019 гг. неизвестный, используя неидентифицированные вредоносные компьютерные программы, систематически осуществлял массовые распределенные атаки типа «отказ в обслуживании» на информационно-телекоммуникационную сеть ООО «Т», одновременно выдвигая в адрес компании требования о денежных выплатах за прекращение преступных действий.

Описанные действия повлекли несанкционированное блокирование компьютерной информации, находящейся на носителях информации в центрах обработки данных. Установить лицо, подлежащее привлечению в качестве обвиняемого, не представилось возможным, в связи с чем предварительное следствие приостановлено.

---

[1] Приговор Ленинского районного суда г. Пензы от 11.08.2020 № 1-191/2020 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

Непрофессиональное создание, использование и распространение вредоносных компьютерных программ

Для совершения таких преступлений не требуется высокой квалификации в сфере информационных технологий, необходимы лишь базовые навыки пользователя персонального компьютера или иной компьютерной техники.

В производстве СУ УМВД России по г. Краснодару находилось уголовное дело по обвинению В. в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ. Согласно полученным доказательствам В. с целью получения полного функционала продуктов Microsoft Office и Windows без прохождения предусмотренной для этого правообладателем процедуры платной активации, использовал полученную с неустановленного интернет-ресурса вредоносную компьютерную программу – активатор KMSauto, предназначенную для несанкционированной модификации компьютерной информации, а именно нейтрализации средств защиты.

Мошенничество в сфере компьютерной информации

Как и вышеуказанные компьютерные преступления, мошенничество в сфере компьютерной информации по признаку принадлежности субъекта преступления к структурам потерпевшего можно разделить на два вида: внешнее и внутреннее.

Внутреннее мошенничество в сфере компьютерной информации

Данные преступления совершаются работниками или контрагентами организации, против которой направлено криминальное деяние. Средством их совершения выступает обусловленный профессиональной деятельностью доступ к хранению, обработке или передаче компьютерной информации, содержащей сведения о предмете хищения.

ГСУ ГУ МВД России по Ставропольскому краю окончено уголовное дело по обвинению М., Я., К. и С. в совершении преступления, предусмотренного п. «в» ч. 3 ст. 159[6] УК РФ.

Расследованием установлено, что обвиняемые, являясь сотрудниками оператора сотовой связи ПАО «М.», вопреки возложенным на них служебным обязанностям, согласно которым они имели законный доступ к хранящейся в базе данных серверов компании информации об абонентах, путем ввода, модификации компьютерной информации и вмешательства в функционирование средств ее хранения, обработки и передачи, используя автоматизированное программное обеспечение и компьютерные программы, посредством которых производится проверка проблемы зачисления денежных средств на лицевые счета клиентов, осуществили финансовые корректировки остатков лицевых счетов абонентов ПАО «М.» в сторону увеличения, похитив принадлежащие данной организации денежные сред-

ства на общую сумму 694 146 рублей. Приговором Кисловодского городского суда М., Я., К. и С. осуждены к различным срокам лишения свободы[1].

Внешнее мошенничество в сфере компьютерной информации

В отличие от внутреннего мошенничества в преступную деятельность здесь имплементируются более сложные схемы доступа к компьютерной информации, при использовании которой совершается преступление.

СЧ СО УТ МВД России по УрФО в суд направлено уголовное дело по обвинению трех лиц в совершении серии преступлений, предусмотренных ч. 4 ст. 159[6] *УК РФ, по факту хищения денежных средств девяти туристических организаций. Схема хищения выглядела следующим образом: участники организованной преступной группы, используя вредоносное программное обеспечение, получали неправомерный доступ к вычислительной технике туристических агентств, что позволяло им за счет денежных средств данных компаний дистанционно посредством сети «Интернет» приобретать железнодорожные билеты на имена лжепассажиров. Лица, находящиеся в разных городах России, на чьи имена были куплены билеты, сдавали их в железнодорожные кассы, а полученные денежные средства переводили на электронные кошельки злоумышленников. Всего в результате описанных действий обналичено 443 электронных проездных документа на сумму более 8 000 000 рублей.*

Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Количество преступлений, предусмотренных ст. 274[1] УК РФ, ежегодно существенно растет. Так, если в 2021 г. было зарегистрировано 159 таких преступлений, то в 2022 г. их насчитывалось уже 519. В практике следственных подразделений органов внутренних дел наиболее распространенными примерами таких криминальных деяний являются факты неправомерного доступа к Федеральному регистру вакцинированных от COVID-19 и базам данных операторов связи, которые отнесены к объектам критической информационной инфраструктуры РФ.

Приговором Абаканского городского суда от 29 июля 2020 г. № 1-805/2020 К. осужден по ч. 2 ст. 274[1] УК РФ к наказанию в виде 2 лет лишения свободы условно, с испытательным сроком 2 года[2]*. Преступные действия К. выразились в том, что он, являясь сотрудником ПАО «МТС», в нарушение нормативных документов, регламентирующих порядок обращения к базам*

---

[1] Приговор Кисловодского городского суда Ставропольского края от 03.09.2021 № 1-29/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

[2] Приговор Абаканского городского суда от 29.07.2020 № 1-805/2020 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

данных, содержащих детализацию оказания услуг абонентам оператора сотовой связи, за вознаграждение от неустановленного следствием лица осуществлял неправомерный доступ к охраняемой законом вышеуказанной компьютерной информации и копировал ее.

Квалификация действий К. по ст. 274[1] УК РФ, а не по ст. 272 УК РФ обусловлена тем, что ПАО «МТС» является субъектом критической информационной инфраструктуры РФ, а информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, принадлежащие данной организации, – объектами критической информационной инфраструктуры. Подобными умозаключениями аргументируется практика квалификации преступлений, связанных с внесением недостоверной информации в Федеральный регистр вакцинированных от COVID-19.

Приговором Кизилюртовского городского суда Республики Дагестан от 23 декабря 2021 г. № 1-148/2021 М. осужден по ч. 4 ст. 272 УК РФ к наказанию в виде лишения свободы сроком на 3 года 6 месяцев условно, с испытательным сроком 2 года[1]. Преступные действия М. выразились в том, что он, являясь программистом отдела информационных технологий Кизилюртовской больницы, осуществил неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в Федеральном регистре вакцинированных от COVID-19, куда внес заведомо ложные сведения о своей вакцинации. Вышеуказанный регистр, являясь информационной системой Министерства здравоохранения РФ, относится к объектам критической информационной инфраструктуры.

Порядок категорирования объектов критической информационной инфраструктуры регламентирован Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», постановлением Правительства РФ от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», приказом Федеральной службы по техническому и экспортному контролю Российской Федерации от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации». Реестр объектов критической информационной инфраструктуры не находится в открытом доступе. Задача по установлению факта внесения определенного объекта в указанный реестр на практике обычно решается путем направления запроса субъекту критической информационной инфраструктуры.

---

[1] Приговор Кизилюртовского городского суда Республики Дагестан от 23.12.2021 № 1-148/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

Правоприменительная практика в сфере уголовного судопроизводства не характеризуется единообразием. Схожие по фактическим обстоятельствам деяния могут квалифицироваться по-разному даже в рамках одного субъекта РФ. Преступления в сфере компьютерной информации не являются исключением. В рамках данного учебного пособия авторским коллективом предпринята попытка унификации подходов к юридической квалификации рассматриваемой категории криминальных деяний в практике подразделений предварительного следствия органов внутренних дел. Для демонстративности наиболее проблемные вопросы, выявленные в результате изучения обвинительных заключений, приговоров и иных процессуальных документов, объединены в условные группы.

Проблемы квалификации неправомерного доступа к учетным записям пользователей интернет-ресурсов и последующих хищений

В большинстве субъектов РФ сложилась практика квалификации подобных деяний как совокупности преступлений: по ч. 2 ст. 272 УК РФ за неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности, и по соответствующей статье УК РФ за последующее хищение.

В производстве СУ УМВД России по Оренбургской области находилось уголовное дело по обвинению М. в совершении ряда преступлений, предусмотренных ч. 2 ст. 272 и ч. 1 и 2 ст. 159 УК РФ. Согласно полученным доказательствам М., имея умысел на хищение денежных средств граждан, используя заранее приобретенные логины и пароли, осуществил неправомерный доступ к персональным страницам пользователей социальной сети, после чего изменил их, тем самым заблокировав компьютерную информацию для законных владельцев учетных записей. Затем, действуя от имени последних, направил их подписчикам сообщения с просьбой одолжить денежные средства. Получатели указанных писем, будучи введенными в заблуждение относительно авторства сообщения, перечисляли различные суммы на подконтрольные М. счета. Преступными действиями М. потерпевшим причинен материальный ущерб в размере 180 000 рублей.

В ходе анализа правоприменительной практики, проведенного в рамках подготовки учебного пособия, выявлено, что в ряде регионов сформирован другой подход к решению данного юридического вопроса. Так, в соответствии с информацией, направленной СУ МВД по Республике Бурятия, позиция прокуратуры заключается в рассмотрении неправомерного доступа к учетным записям пользователей интернет-ресурсов как способа совершения мошенничества, данное деяние дополнительно по ст. 272 УК РФ не квалифицируется.

Аналогичной позиции придерживается ГСУ МВД по Республике Татарстан. Здесь, в отличие от предыдущего субъекта, эта позиция идет вразрез с мнением местного надзорного ведомства по данному вопросу. С точки зрения прокуратуры Республики Татарстан мошенничества,

связанные со взломом страницы в социальных сетях, должны квалифицироваться не только по ст. 159 УК РФ, но и по ст. 272 УК РФ. Однако орган предварительного следствия с данной позицией не согласен, обосновывая это тем, что аккаунты в социальных сетях не относятся к категории охраняемой законом компьютерной информации, поскольку не представляют ни государственную, ни коммерческую тайну. Все персональные данные, которые размещаются на таких страницах, являются общедоступными в силу п. 2 ч. 2 ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в связи с чем применение такого понятия, как тайна связи и ст. 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», невозможно.

Подобную, по мнению авторского коллектива, ошибочную позицию можно встретить и в правоприменительной практике других регионов РФ.

В ходе предварительного следствия по уголовному делу, возбужденному СУ МВД по Республике Адыгея по ч. 2 ст. 272 УК РФ, установлено, что неизвестное лицо в 2021 г. путем подбора логина и пароля от аккаунта в социальной сети Instagram и электронного почтового ящика ООО «Мэйл.Ру», принадлежащих С., заблокировало правомерный доступ последней к указанным учетным записям с целью публикаций не соответствующих действительности сведений о сборе денежных средств. Довести свой преступный умысел до конца неустановленное лицо не смогло по не зависящим от него обстоятельствам. В связи с позицией прокуратуры об ошибочности отнесения содержащейся в аккаунте социальной сети и электронном почтовом ящике информации к категории охраняемой законом данное преступление переквалифицировано на ч. 3 ст. 30, ч. 1 ст. 159[6] УК РФ.

Приведенная аргументация противоречит требованиям закона и сложившейся на большей части России юридической практике. В соответствии со ст. 23 Конституции РФ каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, а также право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Очевидно, что нарушение данных прав человека происходит при неправомерном доступе к учетной записи в социальных сетях, где содержится как личная информация, так и переписка пользователя с иными лицами. Соответственно, подобная информация охраняется законом. Согласно законодательству и юридической доктрине, вышеуказанные преступные действия следует квалифицировать как совокупность преступлений, предусмотренных ч. 30 ст. 30, ч. 2 ст. 272 и соответствующей частью ст. 159 УК РФ.

Вопрос об отнесении компьютерной информации к категории охраняемой законом крайне важен при квалификации компьютерных преступлений, поскольку данное обстоятельство является обязательным признаком объективной стороны преступлений, предусмотренных ст. 272 УК РФ. В связи с этим в приложении 2 настоящего пособия представлен перечень нормативных правовых актов, относящих сведения к категории ограниченного доступа.

Имущественные преступления, следующие за неправомерным доступом к учетным записям пользователей интернет-ресурсов, не всегда осуществляются в виде мошеннических действий.

В производстве СУ УМВД России по Тамбовской области находилось уголовное дело по обвинению П. в совершении серии преступлений, предусмотренных ч. 1 ст. 272 и ч. 1 ст. 163 УК РФ. Установлено, что в 2020 г. П. путем введения полученных при неустановленных обстоятельствах логинов и паролей осуществил неправомерный доступ к закрытой информации страниц граждан в социальной сети «ВКонтакте», после чего произвел копирование частных видеозаписей, изображений и переписки их владельцев. Далее, под угрозой распространения указанных сведений, позорящих потерпевших и способных причинить существенный вред их правам и законным интересам, путем переписки П. незаконно требовал перевести ему денежные средства в различных суммах на принадлежащий ему счет биткоин-кошелька. Ленинским районным судом г. Тамбова уголовное дело в отношении П. прекращено по ст. 25[1] УПК РФ с назначением судебного штрафа[1].

В приведенном примере квалификация действий обвиняемого, связанных с неправомерным доступом к компьютерной информации, представляется ошибочной, поскольку в деяниях прослеживается корыстная заинтересованность. Соответственно, их необходимо квалифицировать по ч. 2 ст. 272 УК РФ.

Проблемы квалификации киберпреступлений, связанных с шифрованием компьютерной информации и последующими требованиями о выкупе паролей для расшифровки

Как упоминалось выше в данной главе, преступления, связанные с шифрованием компьютерной информации и последующим требованием выкупа за ее расшифровку, имеют широкое распространение во всем мире. Органы предварительного следствия в системе МВД России квалифицируют такие преступления по ст. 272 или 273 УК РФ.

23.07.2020 СУ УТ МВД России по СЗФО возбуждено уголовное дело по ч. 2 ст. 273 УК РФ в отношении неустановленного лица, которое распространило вредоносное программное обеспечение, а также выполнило несанкционированное кодирование и блокировку информации, находящейся в персональном компьютере АО «К», нарушив деятельность предприятия. В последующем в АО «К» посредством электронной почты поступило предложение неустановленного лица о приобретении программного обеспечения, позволяющего разблокировать закодированную информацию за криптовалюту, эквивалентную 4000 долларов США. В ходе расследования устано-

[1] Постановление Ленинского районного суда г. Тамбова от 27.05.2021 № 1-129/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

вить лицо, подлежащее привлечению в качестве обвиняемого, не представилось возможным, в связи с чем предварительное следствие приостановлено.

Принципиальным обстоятельством, влияющим на выбор конкретной нормы права, является способ проникновения в компьютерную инфраструктуру потерпевшего. Если доступ к информации совершен посредством приобретения необходимых для этого сведений (IP-адреса, логина, пароля и др.) на сторонних интернет-ресурсах, а затем они использованы в обычном для всех пользователей порядке через сеть «Интернет» без применения каких-либо вредоносных программ (пример см. ранее[1]), то содеянное квалифицируется по ч. 2 ст. 272 УК РФ. Если же доступ к информации, которую злоумышленник планирует зашифровать, осуществляется посредством использования вредоносной программы, то деяние подпадает под действие ч. 2 ст. 273 УК РФ.

В последнем случае ст. 273 УК РФ охватываются лишь действия по использованию компьютерной программы, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. При этом упускаются из виду действия преступника по неправомерному доступу к охраняемой законом информации и общественно опасные последствия в виде блокирования данной информации. Таким образом, квалификация действий шифровальщиков-вымогателей по ст. 272 УК РФ представляется необходимой во всех случаях. Если для неправомерного доступа использовалась вредоносная программа, то деяние следует квалифицировать как совокупность преступлений и дополнительно вменять ст. 273 УК РФ.

Другим проблемным моментом в квалификации данных преступлений является определение юридической природы требований о выкупе паролей или иных средств для возобновления доступа к зашифрованной информации. Такие действия не охватываются ст. 272 или 273 УК РФ, в связи с чем требуют отдельной правовой оценки.

На первый взгляд подобные факты схожи с составом преступления, предусмотренного ст. 163 УК РФ, однако объективная сторона вымогательства не предусматривает требования передачи чужого имущества под угрозой уничтожения или блокирования компьютерной информации. Таким образом, можно говорить о правовом пробеле, так как рассматриваемые общественные отношения не урегулированы в достаточной степени. Преодоление данного пробела предпринималось правоприменительной практикой.

В производстве следственного подразделения УМВД России по Томской области находилось уголовное дело, расследование которого показало, что Д., используя приобретенные им логины и пароли к администра-

[1] Приговор Армавирского городского суда Краснодарского края от 28.09.2021 № 1-469/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

тивным учетным записям ООО «Л», осуществил неправомерный доступ к охраняемой законом компьютерной информации, принадлежащей данной организации. После этого, применяя специализированное программное обеспечение, обвиняемый произвел блокирование указанной информации путем ее шифрования и направил электронное письмо в адрес ООО «Л», в котором под угрозой сохранения блокировки, уничтожения и повреждения компьютерных систем организации выдвинул требования о перечислении ему 2 биткоинов, что эквивалентно 1 261 838,3 рубля. В ходе переписки с представителем ООО «Л» Д. согласился предоставить ключи для снятия блокировки серверов за 0,8 биткоина, то есть за 504 640 рублей. После получения указанного имущества Д. предоставил ключи для расшифровки компьютерной информации. Его действия квалифицированы по ч. 4 ст. 272, п. «б» ч. 3 ст. 163 УК РФ[1].

Данный пример является показательным, поскольку убедительно демонстрирует высокую общественную опасность описанного вида преступлений. Необходимость квалификации подобных деяний как совокупности неправомерного доступа к компьютерной информации и соответствующего преступления против собственности представляется очевидной, однако в связи с принципом законности практическая реализация данной идеи на сегодняшний момент возможна только в единичных случаях.

По мнению авторского коллектива, единственно верным способом преодоления выявленного пробела в праве является внесение соответствующих изменений в ст. 163 УК РФ.

Проблемы соотношения ст. 159 и 159[6] УК РФ

В правоприменительной практике органов предварительного следствия МВД России нередко встречается неправильное разграничение мошенничества, предусмотренного ст. 159 УК РФ, и мошенничества в сфере компьютерной информации, предусмотренного ст. 159[6] УК РФ.

В 2021 г. СУ УМВД России по Калужской области завершено уголовное дело по ч. 1 ст. 159[6], ч. 2 ст. 272 УК РФ.

Установлено, что в 2019–2020 гг. Э., действуя с целью хищения денежных средств пользователей сети «Инстаграмм», зная логин и пароль одного из аккаунтов, осуществил вход в него, после чего произвел замену пароля для последующего доступа к нему, тем самым заблокировав компьютерную информацию для ее законного владельца. Далее от имени владельца указанной учетной записи направил ее знакомой Х. сообщение с просьбой одолжить денежные средства в сумме 7 000 рублей, которые последняя, будучи введенной в заблуждение относительно авторства просьбы, перевела на подконтрольный Э. банковский счет. Сухиничским районным судом Калужской

[1] Приговор Советского районного суда г. Томска от 23.05.2022 № 1-31/2022 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

области уголовное дело в отношении Э. прекращено по основанию, предусмотренному ст. 25 УПК РФ[1].

Квалификация действий Э., связанных с хищением денежных средств, представляется спорной. В соответствии с п. 20 постановления Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в сети «Интернет», то такое мошенничество следует квалифицировать по ст. 159, а не ст. 159^6 УК РФ.

Способом совершения мошеннических действий, предусмотренным ст. 159^6 УК РФ, является не обман или злоупотребление доверием, а вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Под таким вмешательством следует понимать целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него. Примеры таких преступлений приведены в данной главе выше.

Проблемные вопросы правоприменительной практики по расследованию преступлений в сфере компьютерной информации

Институт возбуждения уголовного дела в российском уголовном процессе играет роль своеобразного фильтра, позволяющего отсеивать деяния, которые в соответствии с уголовным законом не являются преступлениями. На данной стадии в том числе необходимо проверять, является ли лицо, совершившее преступные действия, субъектом преступления.

21 апреля 2021 г. СО ОМВД России по г. Ухте (МВД по Республике Коми) возбуждено уголовное дело по ч. 2 ст. 272 УК РФ по факту внесения неустановленным лицом в электронный журнал одной из школ города ложной информации об оценках учащихся 5-го «А» класса.

При допросе ученика этого класса, мобильный телефон которого использовался для входа в учетную запись преподавателя и исправления отметок, он признался, что логин и пароль подсмотрел у учителя, модификацию информации произвел по причине получения неудовлетворительной

[1] Постановление Сухиничского районного суда Калужской области от 16.04.2021 № 1-4-38/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

оценки. В сентябре 2021 г. уголовное дело прекращено в связи с недостижением виновным возраста уголовной ответственности, то есть на основании п. 2 ч. 1 ст. 24 УПК РФ.

Безусловно, не всегда возможно в ходе проверки сообщения о преступлении установить лицо, его совершившее, однако в данном случае достаточной стала бы своевременная проверка IP-адреса, с которого осуществлен неправомерный доступ к электронному журналу.

Кроме того, на совершение деяния лицом, не достигшим возраста 16 лет, указывали фактические обстоятельства, а именно: исправление оценок в журнале 5-го класса. Данные выводы носят вероятностный характер. На основании предположений не может быть вынесено постановление об отказе в возбуждении уголовного дела, но эти предположения должны являться основанием для более тщательной проверки сообщения о преступлении. Также вызывает сомнение квалификация по ч. 2 ст. 272 УК РФ как совершенного из корыстной заинтересованности. Содержание данного квалифицирующего признака в законе не раскрывается, однако юридическая наука и практика под корыстной заинтересованностью понимают стремление лица путем совершения неправомерных действий получить для себя или других лиц выгоду имущественного характера[1].

Еще одной проблемой являются провокации совершения преступления сотрудниками, осуществляющими оперативно-розыскную деятельность.

Например, *следователем СУ УТ МВД России по ПФО окончено уголовное дело по обвинению Б. в совершении преступлений, предусмотренных ч. 3 ст. 30, ч. 2 ст. 146, ч. 3 ст. 30 ч. 1 ст. 273 УК РФ.*

Предварительным расследованием установлено, что Б. в 2020 г. разместил на торговой интернет-площадке «Авито» объявление об установке и переустановке операционной системы Windows и установке дополнительных систем с выездом на дом. Затем, выполняя заказ одного и своих клиентов, из сети «Интернет» скопировал (приобрел) с целью сбыта и перенес на оптический диск контрафактный инсталляционный экземпляр узкоспециализированной компьютерной программы, а также файлы, предназначенные для нейтрализации путем модификации информации установленных правообладателем средств ее защиты. Далее указанный оптический диск, содержащий контрафактную продукцию и вредоносную компьютерную программу, Б. реализовал участвовавшему в проведении оперативно-розыскного мероприятия «проверочная закупка» Ш. за 500 рублей. В связи с тем, что приобретение программного продукта проводилось под контролем правоохранительных органов лицом, осуществляющим проверочную закупку, преступления Б. не были доведены до конца по независящим от него обстоятельствам.

---

[1] См.: О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий: постановление Пленума Верховного Суда РФ от 16.10.2009 № 19 (п. 16). Доступ из СПС «КонсультантПлюс» (дата обращения: 10.03.2023).

Бугульминский городской суд Республики Татарстан счел обвинение, предъявленное Б., несостоятельным, поскольку собранные по уголовному делу доказательства свидетельствуют, что участвующий в проверочной закупке Ш. сам попросил Б. скачать программу, указав ее название. Следовательно, инициатива по установке программы исходила не от Б., а от Ш.

Таким образом, суд пришел к выводу, что умысел на совершение указанных преступлений у Б. возник в результате деятельности оперативных сотрудников, что является нарушением требований ст. 5 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности». В результате Б. признан невиновным и оправдан приговором суда[1].

Кроме того, вызывает сомнения правильность квалификации действий Б. как покушения на преступление.

Так, юридической практикой, основывающейся на законе и актах официального толкования норм права, факт совершения преступления с формальным составом под контролем правоохранительных органов не влияет на его квалификацию как оконченного.

Например, согласно п. 13 постановления Пленума Верховного Суда РФ от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» получение или дача взятки, если указанные действия осуществлялись в условиях оперативно-розыскного мероприятия, должны квалифицироваться как оконченное преступление вне зависимости от того, были ли ценности изъяты сразу после их принятия должностным лицом либо лицом, выполняющим управленческие функции в коммерческой или иной организации. Аналогичные позиции можно встретить и в других правоинтерпретационных актах[2].

В декабре 2022 г. Пленум Верховного Суда РФ дал разъяснения по некоторым вопросам судебной практики по уголовным делам о преступлениях в сфере компьютерной информации. Позиция авторского коллектива по данным вопросам, изложенная в настоящей главе учебного пособия, в полной мере соответствует содержанию данного правоинтерпретационного акта[3].

---

[1] Приговор Бугульминского городского суда Республики Татарстан от 29.12.2021 № 1-235/2021 // Интернет-ресурс «Судебные и нормативные акты РФ» (СудАкт). URL: https://sudact.ru/ (дата обращения: 13.01.2023).

[2] См.: О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами: постановление Пленума Верховного Суда РФ от 15.06.2006 № 14 (п. 13.1). Доступ из СПС «КонсультантПлюс» (дата обращения: 10.03.2023); О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем: постановление Пленума Верховного Суда РФ от 07.06.2015 № 32 (п. 8). Доступ из СПС «КонсультантПлюс» (дата обращения: 10.03.2023).

[3] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // Бюллетень Верховного Суда РФ. 2023. № 3.

Вопросы для самоконтроля

1. Какие виды преступлений, связанных с неправомерным доступом к компьютерной информации, можно выделить? Приведите примеры.
2. Как следует квалифицировать преступные действия, связанные со взломом учетной записи лица в социальной сети и последующим размещением от имени данного лица сообщений с просьбой перевода денежных средств?
3. Дайте уголовно-правовую оценку киберпреступлениям, связанным с шифрованием компьютерной информации и последующими требованиями о выкупе паролей для расшифровки.
4. Как соотносятся преступления, предусмотренные ст. 159 и 159^6 УК РФ?
5. Назовите виды преступлений, связанные с созданием, использованием и распространением вредоносных компьютерных программ. Приведите примеры.

ГЛАВА 3. ПРОЦЕССУАЛЬНЫЕ И КРИМИНАЛИСТИЧЕСКИЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ И ИНЫХ ПРОЦЕССУАЛЬНЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Деанонимизация в сети «Интернет» следственным путем

В настоящее время значительная доля преступлений совершается с использованием сети «Интернет», что обусловливает трансграничный характер следов криминальной деятельности даже в тех случаях, когда преступник и потерпевший находятся на территории РФ. Одной из ключевых проблем противодействия данному виду преступлений является использование злоумышленниками для конспирации преступной деятельности так называемых средств подмены истинного IP-адреса. Базовые методы работы с IP-адресами достаточно давно усвоены правоохранителями, однако, когда дело касается современных средств анонимизации личности в сети «Интернет» (подробнее см. в главе 1), возникают серьезные и порой непреодолимые трудности.

В ходе подготовки учебного пособия проведено интервьюирование 48 сотрудников органов внутренних дел, проходящих службу в различных регионах РФ, чья деятельность связана с противодействием киберпреступлениям. В ходе опроса выяснялось, известны ли респондентам вышеуказанные средства анонимизации личности в сети «Интернет»; есть ли возможность их преодолеть; известны ли такие средства преодоления, как использование cookie-файлов и отпечатков браузера. Все респонденты заявили, что знают такие способы подмены IP-адреса, как прокси-серверы, VPN-сервисы, сеть «Tor». Способ деанонимизации абонентского устройства пользователя с помощью cookie-файлов известен 13 опрошенным, тем не менее случаев его успешного применения нет. Также все интервьюируемые высказали мнение об отсутствии способов установления истинного IP-адреса пользователя, который использует зарубежный VPN, поскольку подобные сервисы не отвечают на запросы российских правоохранителей.

В связи с обозначенной проблематикой далее будут рассмотрены возможные способы преодоления сокрытия истинного IP-адреса пользователя сети «Интернет». В науке подобные вопросы неоднократно подвергались исследованию, однако в большей степени данные научные труды посвящены технической стороне вопроса[1]. В связи с тем, что большинство сотрудников органов внутренних дел, задействованных в вопросах противодействия киберпреступности, имеют юридическое, а не специальное обра-

[1] См., например: *Зулькарнеев И. Р., Козлов А. Е., Нестор В. О.* Деанонимизация правонарушителей в сети Интернет // Электронные средства и системы управления: материалы докладов Международной научно-практической конференции. 2019. № 1-2. С. 119–122; *Шелудяков Д. А., Корчагин С. А., Сердечный Д. В.* Исследование способов деанонимизации пользователей VPN-сервисов. Саратов, 2021.

зование, они сталкиваются с трудностями, связанными с пониманием технических материалов и их практической реализацией. Авторским коллективом предпринята попытка адаптировать имеющиеся в технических науках знания по деанонимизации личности в сети «Интернет» для использования их в повседневной служебной деятельности следователями.

Деанонимизация пользователей виртуальной частной сети через иные сайты

Упрощенно работу виртуальной частной сети можно представить следующим образом. Пользователь сервиса подключается к интересующему его интернет-сайту не напрямую через своего интернет-провайдера, а через VPN. В связи с этим конечный интернет-ресурс видит лишь IP-адрес VPN, а не истинный IP-адрес пользователя (подробнее см. в главе 1, рис. 5). Соответственно, в ответе на запрос от администратора интернет-сайта правоохранительные органы смогут получить IP-адрес, принадлежащий виртуальной частной сети. При проверке полученного адреса через открытые источники можно установить конкретную организацию, связанную с данной сетью, в которую в дальнейшем возможно направить запрос с целью установления IP-адреса пользователя, однако зачастую подобные сервисы находятся вне юрисдикции РФ, что в большинстве случаев является непреодолимым препятствием.

Для наибольшей наглядности демонстрации метода деанонимизации пользователей VPN через иные сайты смоделируем следственную ситуацию. Допустим, производится расследование по уголовному делу о неправомерном доступе к компьютерной информации – учетной записи в социальной сети «ВКонтакте». Следователь на основании запроса получил информацию об IP-адресах, с которых преступник подключался к учетной записи, однако при их проверке установлено, что они принадлежат VPN-сервису в Королевстве Нидерландов.

В этом случае возможно выдвижение гипотезы, что преступник наравне с совершением указанного преступления и размещением объявления осуществлял параллельные подключения к иным интернет-ресурсам, которые не связаны с его противоправной деятельностью и используются им в повседневной жизни. Например, в рамках того же соединения, в ходе которого взламывал учетную запись на интернет-сайте «ВКонтакте», он мог обращаться к своей электронной почте, учетным записям в социальных сетях, интернет-банкингу и др. В таком случае все эти сетевые ресурсы так же, как и указанная социальная сеть, видели один и тот же IP-адрес, принадлежащий виртуальной частной сети. Для проверки гипотезы необходимо направление запросов в наиболее распространенные интернет-сервисы с вопросом, обращался ли к ним в орган следствия в интересующее время пользователь с IP-адреса, принадлежащего VPN. В случае положительного ответа можно получить сведения об иных учетных записях лица на сторонних интернет-сайтах, которые способны привести к уста-

новлению личности преступника. Данный способ также работает для деанонимизации пользователей сети «Тор».

Однако здесь следует учитывать два важных фактора. Во-первых, IP-адрес, предоставляемый пользователю VPN, является динамическим, то есть выдается лишь на одну сессию сетевого подключения. Соответственно, при направлении запросов на сторонние интернет-сайты необходимо указывать ограниченный период времени использования адреса (например, 30 минут до и 30 минут после времени, указанного в ответе на запрос от социальной сети «ВКонтакте»). Во-вторых, в настоящее время распространена NAT-адресация, когда один и тот же IP-адрес предоставляется множеству (до сотен и тысяч) пользователей (подробнее о NAT см. в главе 1).

Деанонимизация пользователей виртуальной частной сети путем сопоставления соединений

Воспользуемся следственной ситуацией из предыдущего метода деанонимизации. В рамках данного метода источником информации будет являться не конечный сетевой ресурс, к которому потенциально мог обращаться пользователь, а интернет-провайдер, через которого лицо подключалось к виртуальной частной сети. Гипотеза следующая: преступник подключался к VPN через отечественного интернет-провайдера и последнему известен истинный IP-адрес пользователя. Для проверки гипотезы необходимо направление запросов о предоставлении информации всем действующим интернет-провайдерам с вопросом о том, осуществлялось ли их клиентами в интересующее орган следствия время подключение к IP-адресу, принадлежащему VPN. В случае положительного ответа следователь получит сведения об абоненте, который пользовался виртуальной частной сетью.

Приведенный способ также не следует идеализировать, в связи с чем необходимо учитывать следующие обстоятельства: во-первых, фигурирующий в материалах уголовного дела VPN-сервис может быть популярным и одновременно к нему могут подключаться множество пользователей; во-вторых, когда преступник использует цепочку VPN, деанонимизировать его данным способом не получится.

Деанонимизация пользователей с использованием cookie-файлов

Упрощенно cookie-файл можно условно представить как уникальный номер, который интернет-сайт присваивает веб-браузеру при первом обращении[1]. При использовании такого номера веб-браузер будет идентифицировать себя перед интернет-сайтом во всех последующих соединениях. Удобство использования cookie-файлов заключается в том числе в отсутствии необходимости у пользователей каждый раз проходить процедуру

[1] Что такое файлы cookies? URL: https://trends.rbc.ru/trends/industry/5f4e8d719a794788d1c8b49f (дата обращения: 10.03.2023).

авторизации, вводя свои логин и пароль: интернет-сайт узнает их по используемому веб-браузеру. Таким образом, даже в тех случаях, когда мы выйдем из учетной записи, но будем обращаться к интернет-сайту с того же веб-браузера, он все равно нас идентифицирует.

Реализуя такой метод в рамках вышеобозначенной следственной ситуации, возможно выдвинуть гипотезу: злоумышленник, используя один и тот же веб-браузер, осуществлял подключения к сайту «ВКонтакте» не только в преступных целях, но и для личного пользования. Например, он может иметь свою учетную запись в этой социальной сети, или этот веб-браузер используют члены его семьи для общения на сетевом ресурсе. Для проверки гипотезы необходимо запросить сведения об иных IP-адресах и учетных записях пользователя, подключение к которым происходило при использовании одного веб-браузера, полученные посредством анализа cookie-файлов. К сожалению, анализ может быть проведен только администратором соответствующего веб-сайта, и проверить, действительно ли он проводился по запросу правоохранительных органов, невозможно.

Деанонимизация пользователей с использованием отпечатков браузера

Отпечатками браузера (от англ. *browser fingerprints*) называют информацию в отношении устройства пользователя и его программного обеспечения, которую веб-браузер передает интернет-сайту, в том числе для наиболее правильного отображения запрашиваемых клиентом веб-страниц[1]. К такой информации относится: user-agent (сведения об операционной системе и веб-браузере), часовой пояс, размеры экрана используемого устройства, язык, шрифты, установленные расширения веб-браузера и др. Отдельно взятый элемент указанной информации не является уникальным и может являться атрибутивным признаком множества пользователей, но в совокупности эти элементы позволяют уникализировать веб-браузеры до небольшой группы или даже до единственного лица.

Все веб-браузеры отправляют схожую информацию на сервер, но ее объем зависит от индивидуальных настроек приватности. Даже наиболее известный среди так называемых анонимных веб-браузеров – Tor-браузер, передает подобную информацию, в связи с чем в руководстве пользователя этого программного продукта не рекомендуется работать из полноэкранного режима с целью предотвращения создания уникального размера экрана. Интернет-сайты аккумулируют указанные сведения в коммерческих целях, а именно для настройки рекламы. В связи с этим предполагается возможным проводить подобную работу по уникализации и идентификации пользователей и по запросам правоохранительных органов.

---

[1] Browser Fingerprint – анонимная идентификация браузеров. URL: https://habr.com/ru/company/oleg-bunin/blog/321294/ (дата обращения: 10.03.2023).

Все приведенные в данной главе методы установления личности пользователя сети «Интернет» не являются идеальными и не дают абсолютных гарантий получения результата. Профессиональный преступник с легкостью может предусмотреть все нюансы, которые помогут ему избежать идентификации таким путем. Однако человеческий фактор здесь играет немаловажную роль: мошенник может быть очень предусмотрительным, продумав все этапы совершения преступления, но из-за невнимательности или легкомыслия совершить грубую ошибку, которая позволит его деанонимизировать. Например, используя цепочку VPN, будучи убежденным в своей невидимости, параллельно с совершением преступления проверит свою электронную почту. Таким образом, следователям в условиях неопределенности недопустимо недооценивать вышеприведенные методы и относиться к ним с предубеждением как к априори неэффективным. Целесообразно использовать каждый возможный шанс раскрытия преступления, каким бы маловероятным он ни казался, а также творчески подходить к решению подобных нетривиальных задач.

Примерная форма запроса, реализующего вышеуказанные методы, приведена в приложении 3.

Осмотр мобильных телефонов

В жизни современного человека смартфон имеет существенное значение, выполняя не только функцию телефона, но и изначально несвойственные ему задачи. Доступность мобильного интернета и развитие технологий позволяет сосредоточить в мобильном устройстве множество различных приложений: социальные сети, мессенджеры, навигационные службы, службы доставки, вызова такси и многое другое. Очевидно, что данная информация может иметь важное криминалистическое значение и являться важным источником доказательств по уголовным делам. Однако здесь присутствуют две проблемы: процессуального и криминалистического характера.

Процессуальный аспект

В смартфоне содержится информация, охраняемая законом, например, переписка в мессенджерах, личные фотографии и иная персональная информация. Является очевидным, что при производстве осмотра данной информации ограничиваются соответствующие права граждан. Согласно ст. 13 УПК РФ ограничение права гражданина на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений допускается только на основании судебного решения. Однако в УПК РФ данный принцип получил реализацию лишь в виде судебного контроля за наложением ареста на почтово-телеграфные отправления. Вопрос получения судебного разрешения для осмотра информации, содержащейся в изъятом мобильном телефоне, является правовым пробелом в условиях наличия вышеуказанного принципа права и отсутствия конкретной правовой

нормы, реализующей данный принцип. В ст. 29 УПК РФ среди полномочий суда не указано принятие решения о производстве осмотра содержащихся в мобильном устройстве сведений, составляющих охраняемую законом тайну.

Данный правовой пробел вызывает затруднения у следственных органов при рассмотрении вопроса об использовании конкретных процессуальных средств для решения обозначенной задачи. В целом юридической практикой выработана позиция, согласно которой осмотр мобильного телефона производится по решению следователя, а судебный контроль за данным следственным действием может быть осуществлен в общем порядке, предусмотренном ст. 125 УПК РФ. Основывается данная позиция на определении Конституционного Суда РФ от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 УПК РФ». Согласно описательной мотивировочной части данного правового акта проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения.

Криминалистический аспект

Следственной практикой выработан наиболее оптимальный алгоритм изъятия мобильного телефона с точки зрения наиболее эффективного использования содержащейся в нем информации:

1) выяснение пароля (графического ключа) разблокировки устройства (в противном случае возникнет необходимость назначения судебной экспертизы для решения этой задачи; при этом с учетом отсутствия надлежащего аппаратно-программного обеспечения в значительной доле случаев решить данную задачу не представляется возможным);

2) перевод устройства в режим полета;

3) незамедлительный осмотр информации, хранящейся в памяти устройства (галерея изображений, переписка мессенджеров и др.), с использованием технических средств фиксации информации, имеющей значение для уголовного дела;

4) перевод устройства в нормальный режим;

5) незамедлительный осмотр информации, хранящейся в сети «Интернет», доступ к которой возможен с использованием устройства (файлы, хранящиеся в облачных хранилищах; социальные сети и др.).

Криминалистическое значение информации, содержащейся в мобильных устройствах, зачастую недооценивается следователями, нередко в связи с непониманием возможностей использования личных смартфонов участников уголовного судопроизводства для целей доказывания. При этом значительная часть данной информации уникальна и может быть

получена только единственным способом – осмотром мобильного телефона, поскольку существенная доля мобильных приложений администрируется зарубежными организациями. Кроме того, даже в тех случаях, когда данную информацию можно получить иными способами, осмотр мобильного телефона является среди них наиболее оптимальным по времени. Далее будут приведены конкретные практические примеры использования указанной информации в ходе предварительного расследования.

На рисунке 8 изображено приложение Google Maps, которое автоматически предустановлено на всех смартфонах на операционной системе Android.

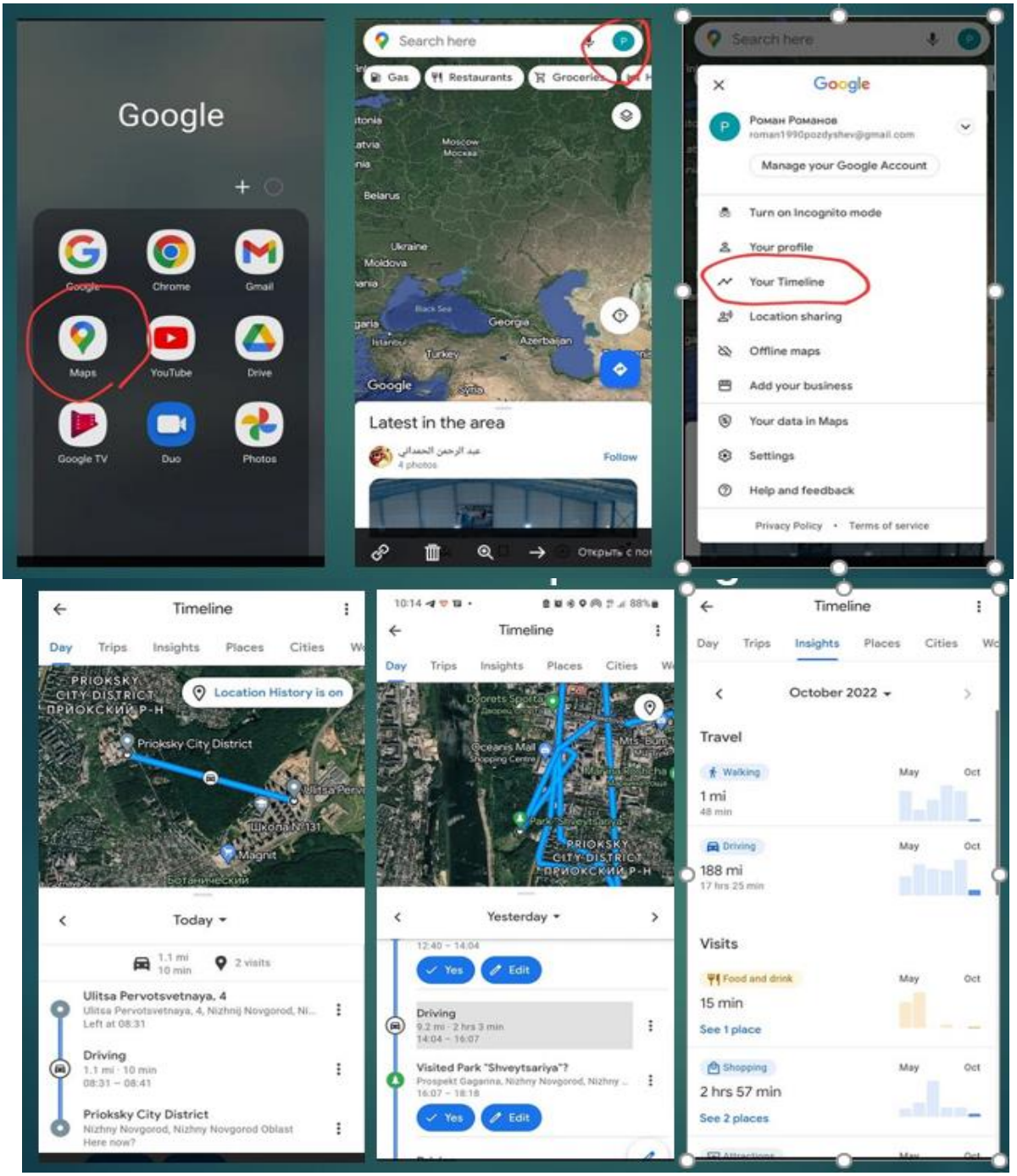

Рис. 8. *Приложение Google Maps*

На смартфонах, работающих на других операционных системах, данное приложение может быть установлено пользователем. Следует сделать оговорку, что в этом примере и далее представлена информация, которую собирают и хранят приложения с настройками по умолчанию. Каждый пользователь может настроить свое устройство индивидуально и при наиболее приватных настройках значительная доля информации, приведенная в главе, не будет обнаружена при осмотре. Однако следует заметить, что большинство пользователей используют приложения с базовыми настройками. В приведенном на рисунке приложении во вкладке «Хронология» можно изучить историю передвижения пользователя за все время существования его учетной записи Google, в том числе работавшей на других устройствах. Возможно сделать выборку информации по дате, месту, а также получить различные аналитические данные.

На рисунке 9 изображено приложение «ВКонтакте». В данном приложении, кроме очевидных способов получения информации о профиле пользователя и его переписке, можно получить информацию о подключениях к учетной записи: IP-адрес, дата и время, место, сведения об устройстве. Данная информация имеет существенную ценность при проверке фактов неправомерного доступа к учетной записи социальной сети «ВКонтакте» и дает возможность оперативно получить сведения, позволяющие установить личность преступника.

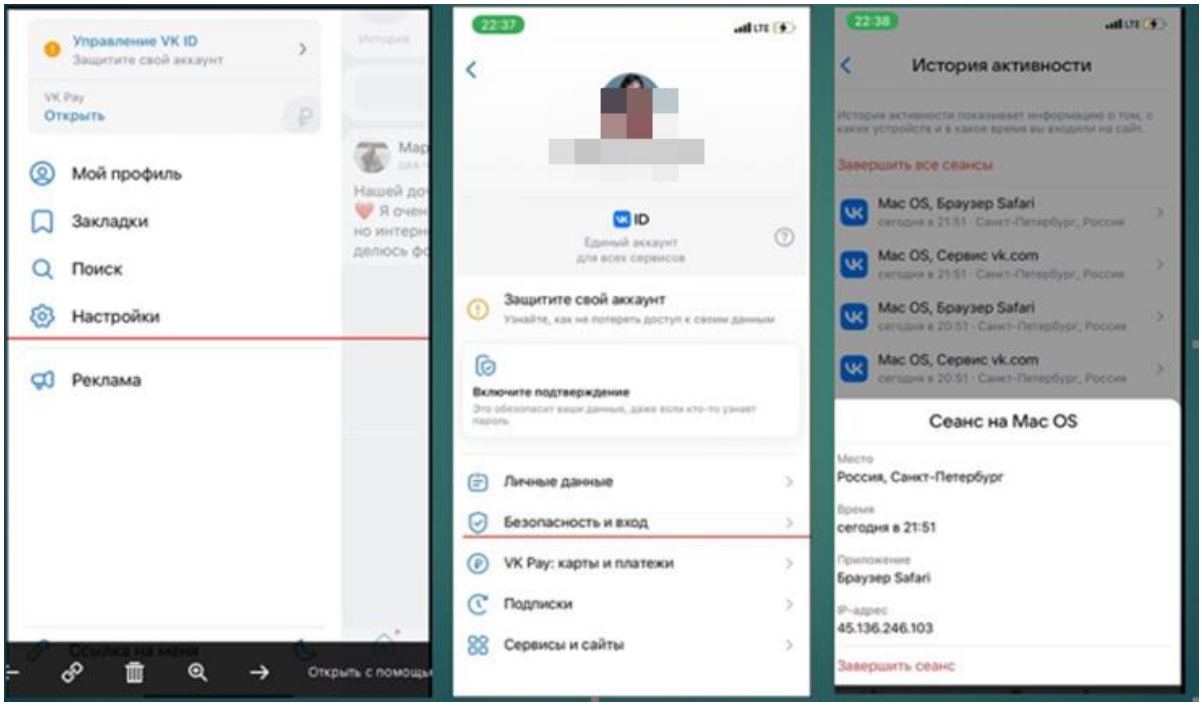

Рис. 9. *Приложение «ВКонтакте»*

Целью настоящей главы не является обзор всех приложений смартфонов, с помощью которых может быть получена криминалистически значимая информация. Она является недостижимой в связи с появлением новых мобильных приложений, обновлением интерфейса и возможностей старых.

Существует множество полезных для следователей приложений: различные карты, социальные сети, онлайн-банки, операторы связи, маркетлейсы и др. Цель приведенной информации – продемонстрировать широкие возможности данного источника доказательств и сориентировать следователей на использование творческого подхода к осмотру мобильных устройств и анализ всех приложений, установленных на смартфоне.

Использование специальных знаний при расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий

Специфика преступлений в сфере компьютерной информации, профессиональная подготовка преступников в сфере информационных технологий, а также отсутствие такой подготовки у следователей обусловливают необходимость в использовании специальных знаний в данной области при расследовании криминальных деяний в киберпространстве.

Производство компьютерной судебной экспертизы является проблемным вопросом для органов предварительного следствия органов внутренних дел на подавляющей территории страны. Это обусловлено множеством обстоятельств. Не во всех регионах есть соответствующие экспертные специальности в подразделениях МВД России, а там, где они есть – существует проблема длительного производства экспертиз и их низкого уровня эффективности. По этим причинам органы предварительного следствия вынуждены назначать экспертизы в негосударственных экспертных учреждениях.

В качестве положительных примеров следует отметить случаи назначения экспертиз сотрудникам АО «Лаборатория Касперского» на безвозмездной основе. Подобная практика существует в следственных подразделениях ГУ МВД России по г. Москве, Нижегородской области и СКФО. Заинтересованность АО «Лаборатория Касперского» заключалась в установлении обстоятельств, способствовавших совершению преступления, и способов распространения вредоносных программ для дальнейшего использования в своей деятельности. В связи с этим данной организацией даются положительные ответы на запросы следователей о возможности проведения судебной экспертизы в инициативном порядке, а также об участии в качестве специалистов при производстве следственных действий.

Однако в данном контексте следует напомнить, что в соответствии с п. 60 ст. 5 УПК РФ и п. 2 постановления Пленума Верховного Суда РФ от 21.12.2010 № 28 «О судебной экспертизе по уголовным делам» судебная экспертиза производится государственными судебными экспертами и иными экспертами из числа лиц, обладающих специальными знаниями. К иным экспертам из числа лиц, обладающих специальными знаниями, относятся эксперты негосударственных судебно-экспертных учреждений, а также лица, не работающие в судебно-экспертных учреждениях. Под негосударственными судебно-экспертными учреждениями следует понимать

некоммерческие организации (некоммерческие партнерства, частные учреждения или автономные некоммерческие организации), созданные в соответствии с ГК РФ и Федеральным законом от 12.01.1996 № 7-ФЗ «О некоммерческих организациях», осуществляющие судебно-экспертную деятельность в соответствии с принятыми ими уставами.

Таким образом, назначение проведения судебных экспертиз в коммерческих организациях, в том числе акционерных обществах и обществах с ограниченной ответственностью, формально является нарушением требований уголовно-процессуального доказательства, поскольку коммерческие организации экспертными *учреждениями* являться не могут в силу организационно-правовой формы, в связи с чем данные заключения эксперта могут быть признаны недопустимыми доказательствами. Например, в апелляционном определении от 13.08.2018 по делу № 22-5954/2018 Свердловский областной суд дал оценку и исключил из числа доказательств экспертизу, проведенную коммерческой организацией ООО АНСЭ «Экспертиза»[1].

В связи с изложенным, если лицо, обладающее специальными знаниями, работает в коммерческой организации, то следует назначать провести экспертизу конкретно данному лицу как не работающему в экспертном учреждении и выполнять требования Уголовно-процессуального кодекса (далее – УПК РФ), предусматривающие действия следователя в подобных случаях, в том числе лично разъяснять права и ответственность эксперта.

Одним из способов снижения нагрузки экспертов является использование доэкспертной оценки предметов, изъятых в ходе предварительного расследования. Целями данной оценки являются формулирование вопросов, ставящихся на разрешение эксперта, и определение перечня объектов, подлежащих направлению на экспертизу.

Кроме того, на данном этапе рассматривается возможность решения следственных задач путем осмотра компьютерной техники с участием специалиста, без производства экспертного исследования. Такой способ взаимодействия следственных и экспертно-криминалистических подразделений используется в ряде подразделений МВД России.

Положительным примером является совместная работа следственного и экспертно-криминалистического подразделений ГУ МВД России по г. Санкт-Петербургу и Ленинградской области по уголовному делу, возбужденному по ч. 4 ст. 159 УК РФ по фактам контактного мошенничества.

На доэкспертную оценку было представлено более 340 объектов, изъятых в ходе обысков в местах жительства подозреваемых. По результатам проведенных следственных действий с применением средств компьютерной лаборатории без назначения экспертизы в течение двух суток осмотрены более трехсот сим-карт и шесть мобильных телефонов, получена и

[1] Апелляционное определение Свердловского областного суда от 13.08.2018 по делу № 22-5954/2018. URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=SOUR&n=153324#30TRb5T8F0F0bY75 (дата обращения: 25.12.2023).

закреплена в протоколе осмотра предметов необходимая информация. В результате проведенных мероприятий отобраны только 11 объектов, по которым следователем назначена судебная компьютерная экспертиза. Примененный подход позволил обеспечить наиболее оптимальное использование сил и средств экспертно-криминалистического подразделения, организовать в кратчайший период эффективное исследование информации более чем на 340 электронных объектах.

В качестве примерных вопросов, которые могут быть поставлены перед экспертом, предлагаем следующие:

1. Имеются ли на предоставленном на исследование носителе информации следы работы на интересующем ресурсе конкретного оборудования с IP-адресом (указывать конкретный IP-адрес)?

2. Имеются ли на предоставленном на исследование носителе информации следы работы в сети «Интернет», содержащие информацию о работе с электронными кошельками, криптокошельками?

3. Имеются ли на предоставленном на исследование носителе информации сведения о логинах и паролях доступа к интернет-ресурсам, установленным программам, интернет-кошелькам, системам дистанционного банковского обслуживания? Если да, то какие именно?

4. Какие mac-адреса имеет сетевое оборудование представленных на экспертизу объектов?

5. Имеются ли на предоставленном на исследование носителе информации сведения о человеке с ФИО: <ФИО> (доступ к социальным сетям, переписка, паспортные данные и т. д.)? Если да, то каковы временные атрибуты соответствующих файлов, их содержащих?

6. Имеются ли на предоставленном на исследование носителе информации программы, которые определяются антивирусным программным обеспечением как вредоносные? Если да, то какие у них функциональные возможности, сетевые взаимодействия, способ проникновения и следы работы в системе?

7. Имеются ли на предоставленном на исследование носителе информации компьютерные программы или другая компьютерная информация, которые имеют функциональные возможности скрытно от пользователя копировать информацию, необходимую для аутентификации в операционной системе, но при этом не являются компонентом операционной системы? Если да, то какие у них функциональные возможности, сетевые взаимодействия, способ проникновения в систему и следы работы в системе?

8. Имеются ли на предоставленном на исследование носителе информации средства удаленного администрирования и управления компьютером?

9. Имеются ли в дампе (снимок информации о состоянии компьютерной системы) сетевого трафика сетевые соединения от/к следующим IP-адресам (перечислить IP-адреса)?

10. Имеется ли на предоставленном на исследование носителе информации программное обеспечение, позволяющее пользоваться услугами

электронной почты? Если да, то какое программное обеспечение (название, версии)?

11. Имеются ли на предоставленном на исследование носителе информации файлы, содержащие электронные почтовые сообщения? О каких электронных почтовых ящиках имеются сведения на предоставленном на исследование системном блоке?

12. Имеется ли на предоставленном на исследование носителе информации программное обеспечение, позволяющее пользоваться услугами мгновенного обмена сообщениями в сети «Интернет»? Если да, то какое программное обеспечение (название, версии)?

Вопросы для самоконтроля

1. Раскройте способ деанонимизации личности преступника, использующего VPN-сервис путем сопоставления соединений.
2. Что такое cookie-файлы и отпечатки браузера? Какое криминалистическое значение они имеют?
3. Раскройте алгоритм изъятия мобильного телефона.
4. Какую криминалистически значимую информацию можно получить при осмотре смартфона?
5. Какие вопросы могут быть поставлены на разрешение компьютерной судебной экспертизы?

ЗАКЛЮЧЕНИЕ

Результаты проведенного авторами по теме учебного пособия исследования позволяют констатировать, что в настоящее время подразделения предварительного следствия органов внутренних дел при расследовании преступлений в сфере компьютерной информации, а также иных преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, сталкиваются с существенными проблемами как уголовно-правового, так и криминалистического характера.

Основными результатами исследования можно назвать следующие.

Во-первых, это анализ и изложение в адаптированном для правоохранительных органов виде криминалистических значимых аспектов информационно-телекоммуникационных технологий и классификация преступлений в сфере компьютерной информации. Данные сведения позволят изучить дедуктивным методом рассматриваемый вопрос и войти в курс дела следователям, не имеющим опыта в данной области.

Во-вторых, уголовно-правовой анализ преступлений в данной сфере и их соотношения друг с другом, что позволит унифицировать подходы правоприменителей к квалификации и обеспечить предсказуемость юридической практики.

В-третьих, криминалистические рекомендации по деанонимизации преступников в сети «Интернет», проведению осмотра мобильных устройств и использованию специальных знаний, которые могут быть полезны в установлении лиц, подлежащих привлечению в качестве обвиняемых по уголовным делам о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий, и собирании доказательств.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты

1. Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 20.12.2022). – Текст : электронный.

2. Гражданский кодекс Российской Федерации. Часть первая : Федеральный закон Российской Федерации от 30 ноября 1994 года № 51-ФЗ : принят Государственной Думой Федерального Собрания Российской Федерации 21 октября 1994 года // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 20.12.2022). – Текст : электронный.

3. Уголовно-процессуальный кодекс Российской Федерации : Федеральный закон Российской Федерации от 18 декабря 2001 года № 174-ФЗ : принят Государственной Думой Федерального Собрания Российской Федерации 22 ноября 2001 года : одобрен Советом Федерации Федерального Собрания Российской Федерации 5 декабря 2001 года // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 20.12.2022). – Текст : электронный.

4. Уголовный кодекс Российской Федерации : Федеральный закон Российской Федерации от 13 июня 1996 года № 63-ФЗ : принят Государственной Думой Федерального Собрания Российской Федерации 24 мая 1996 года : одобрен Советом Федерации Федерального Собрания Российской Федерации 5 июня 1996 года // СПС «КонсультантПлюс» : [сайт]. – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 20.12.2022). – Текст : электронный.

5. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 года № 195-ФЗ : принят Государственной Думой Федерального Собрания Российской Федерации 20 декабря 2001 года : одобрен Советом Федерации Федерального Собрания Российской Федерации 26 декабря 2001 года // СПС «КонсультантПлюс» : [сайт]. – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=414973&dst=100001#m6vO06TCbllVXat11 (дата обращения: 25.12.2022). – Текст : электронный.

Основная литература

6. **Валькова, Т. В**. Расследование преступлений, совершаемых с использованием компьютерных и телекоммуникационных технологий : учебное пособие / Т. В. Валькова, В. В. Долгаев, С. В. Смелова ; МВД России, Санкт-Петербургский университет. – Санкт-Петербург : Изд-во СПб. ун-та МВД России, 2021. – 131, [1] с. – Библиогр.: с. 123–130. – Режим до-

ступа: для авторизир. пользователей. – URL: http://mp.na-mvd.ru/MegaPro/Download/MObject/2881. – ISBN 978-5-91837-408-5 : 0-00. – Текст : электронный.

7. Особенности квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей : учебное пособие / А. Ю. Ушаков, А. Г. Саакян, Р. С. Поздышев, М. А. Степанова ; Министерство внутренних дел Российской Федерации, Нижегородская академия. – Нижний Новгород : НА МВД России, 2022. – 60 с. – (Служим России, служим закону). – Авт. не указаны на тит. л. – Библиогр.: с. 48–53. – Режим доступа: для авторизир. пользователей. – URL: http://mp.na-mvd.ru/MegaPro/Download/MObject/3422. – ISBN 978-5-88840-189-7 : 30-53. – Текст : электронный.

8. Особенности расследования преступлений, совершаемых в сети Интернет с использованием средств анонимизации : методические рекомендации / А. И. Гайдин, Е. А. Пидусов, А. В. Головчанский, Д. В. Гусев ; Воронежский институт МВД России. – Воронеж : Воронеж. ин-т МВД России, 2022. – 42 с. : схем. – (Служим России, служим закону). – Авт. указаны на обороте тит. л. – Библиогр.: с. 40–41. – Режим доступа: для авторизир. пользователей. – URL: http://mp.na-mvd.ru/MegaPro/Download/MObject/3643. – ISBN 978-5-88591-923-4 : 0-00. – Текст (визуальное) : электронный.

Дополнительная литература

9. **Гайдин, А. И.** Практика расследования преступлений, совершаемых с использованием технологий IP-телефонии и программ подмены номеров : методические материалы / А. И. Гайдин, И. С. Звягин, И. С. Садырин ; Воронежский институт МВД России. – Воронеж : Воронеж. ин-т МВД России, 2022. – 35 с. : схем. – Авт. не указаны на тит. л. – Библиогр.: с. 34–35. – Режим доступа: для авторизир. пользователей. – URL: http://mp.na-mvd.ru/MegaPro/Download/MObject/3922. – Текст (визуальное) : электронный.

10. **Коптяев, А. Ю.** Расследование преступлений, совершенных с использованием современных информационно-коммуникационных технологий : учебное пособие / А. Ю. Коптяев ; Министерство внутренних дел Российской Федерации, Тюменский институт повышения квалификации сотрудников МВД России. – Тюмень : ТИПК МВД России, 2022. – 76 с. – Библиогр.: с. 67–70. – Режим доступа: для авторизир. пользователей. – URL: http://mp.na-mvd.ru/MegaPro/Download/MObject/3685. – ISBN 978-5-93160-331-5 : 0-00. – Текст (визуальное) : электронный.

11. **Мещеряков, В. А.** Следы цифрового века / В. А. Мещеряков. – Текст : непосредственный // Вопросы экспертной практики. – 2019. – № S1. – С. 423–426.

12. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации : учебно-методическое пособие /

Э. Д. Нугаева, С. Р. Низаева, В. Р. Гайнельзянова, З. И. Харисова. – Уфа : Уфимский ЮИ МВД России, 2023. – 96 с. – ISBN 978-5-7247-1143-2. – Текст : непосредственный.

13. **Поздышев, Р. С.** Деанонимизация личности преступника в сети «Интернет» / Р. С. Поздышев. – Текст : непосредственный // Вестник Уральского юридического института МВД России. – 2022. – № 2 (34). – С. 50–53.

14. **Поздышев, Р. С.** Основы функционирования сети «Интернет» и ее теневого сегмента / Р. С. Поздышев, Т. И. Гарипов. – Текст : непосредственный // Право и образование. – 2022. – № 3. – С. 56–65.

15. **Поздышев, Р. С.** Структура преступлений в сфере компьютерной информации в практике органов внутренних дел / Р. С. Поздышев, А. Е. Васильев. – Текст : непосредственный // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. – 2022. – № 4 (93). – С. 182–191.

16. **Решняк, О. А.** Расследование хищений чужого имущества, совершенных с использованием информационно-телекоммуникационных технологий : учебное пособие / О. А. Решняк, С. А. Ковалев ; Министерство внутренних дел Российской Федерации, Волгоградская академия. – Волгоград : ВА МВД России, 2021. – 58 с. – Библиогр.: с. 54–58. – URL: http://mp.na-mvd.ru/MegaPro/Download/MObject/2296. – Режим доступа: для авторизир. пользователей. – ISBN 978-5-7899-1282-1 : 0-00. – Текст : электронный.

17. Сфера телекоммуникаций и компьютерной информации как платформа для совершения современных видов преступлений : учебно-практическое пособие / В. И. Алескеров, О. Н. Колокольчикова, Л. В. Василенко, С. Н. Ломакин ; под общей редакцией М. Ю. Литвинова ; МВД России, Федеральное государственное казенное учреждение дополнительного профессионального образования «Всероссийский институт повышения квалификации сотрудников Министерства внутренних дел Российской Федерации». – Домодедово : ВИПК МВД России, 2022. – 359, [1] с. : ил., табл., схем. – Авт. не указаны на тит. л. – Библиогр.: с. 282–285. – Режим доступа: для авторизир. пользователей. – URL: http://mp.na-mvd.ru/MegaPro/Download/MObject/3644. – ISBN 978-5-9552-0775-9 : 0-00. – Текст : электронный.

18. Тактика осмотра компьютерной техники : методические рекомендации / Е. А. Пидусов, В. А. Мещеряков, И. С. Звягин ; Воронежский ин-т МВД России. – Воронеж : Воронеж. ин-т МВД России, 2020. – 28 с. – Библиогр.: с. 27–28. – URL: http://mp.na-mvd.ru/MegaPro/Download/MObject/1830. – Режим доступа: для авторизир. пользователей. – Текст : электронный.

Приложение 1

Интернет-ресурсы даркнета

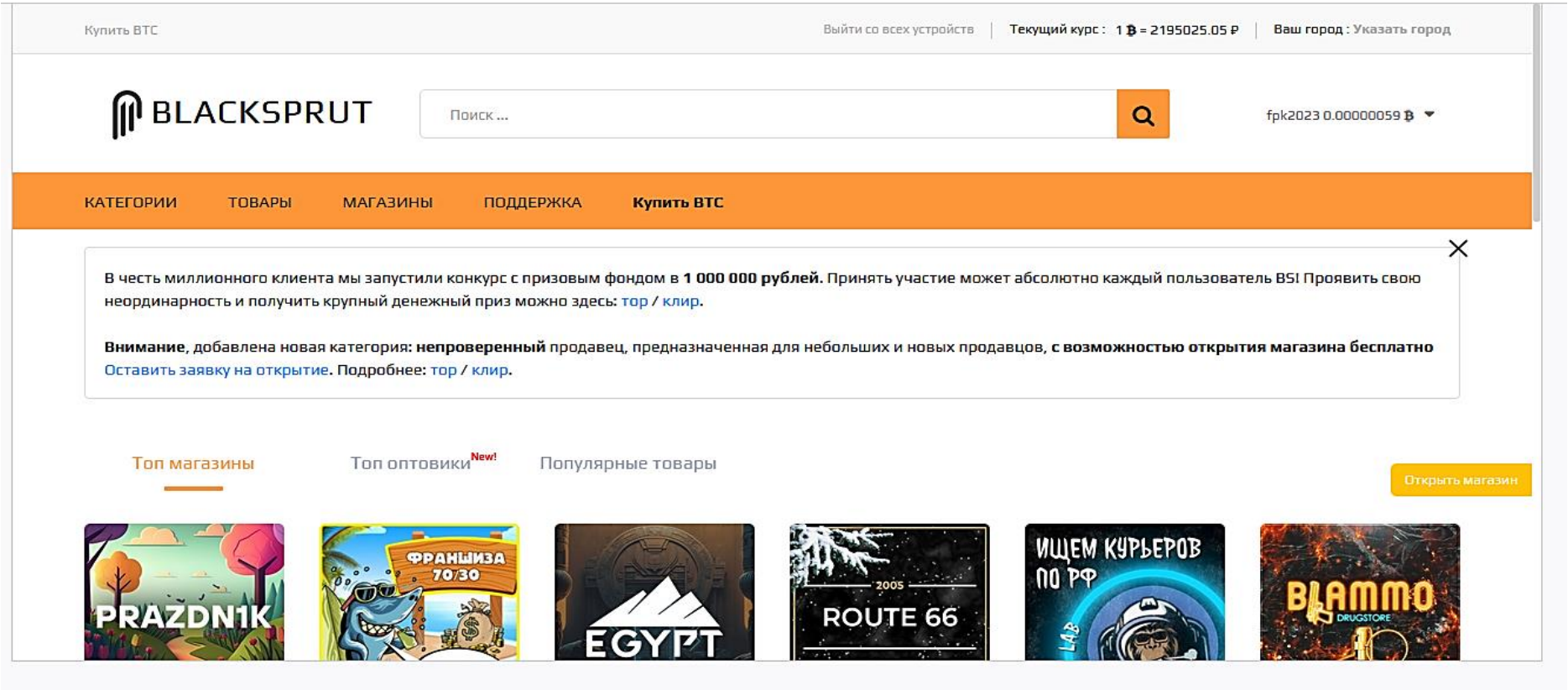

Рис. 1. *Главная страница веб-сайта BlackSprut*

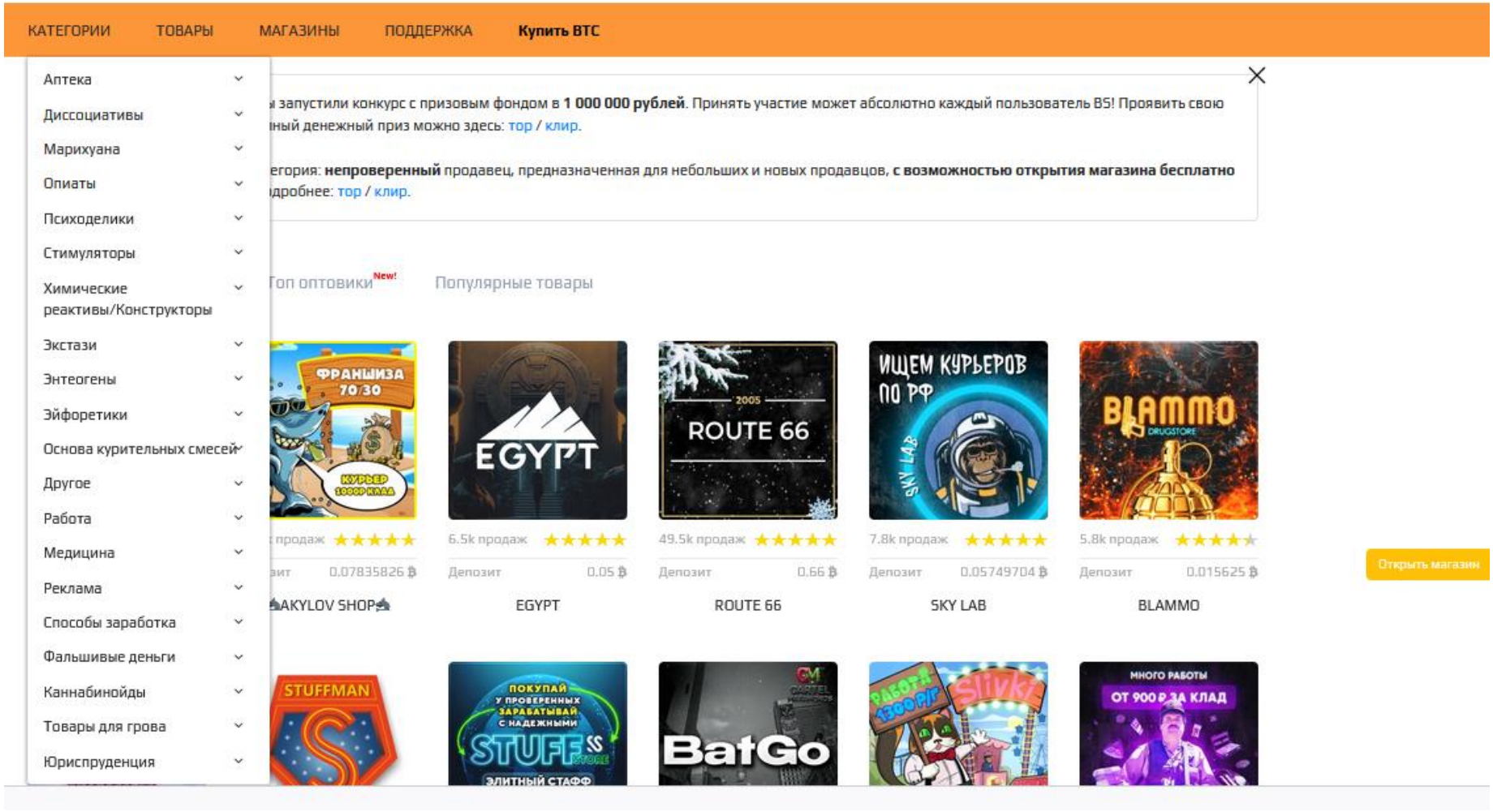

Рис. 2. *Категории товаров (услуг), размещенных на веб-сайте BlackSprut*

Рис. 3. *Витрина магазина по продаже наркотических средств*

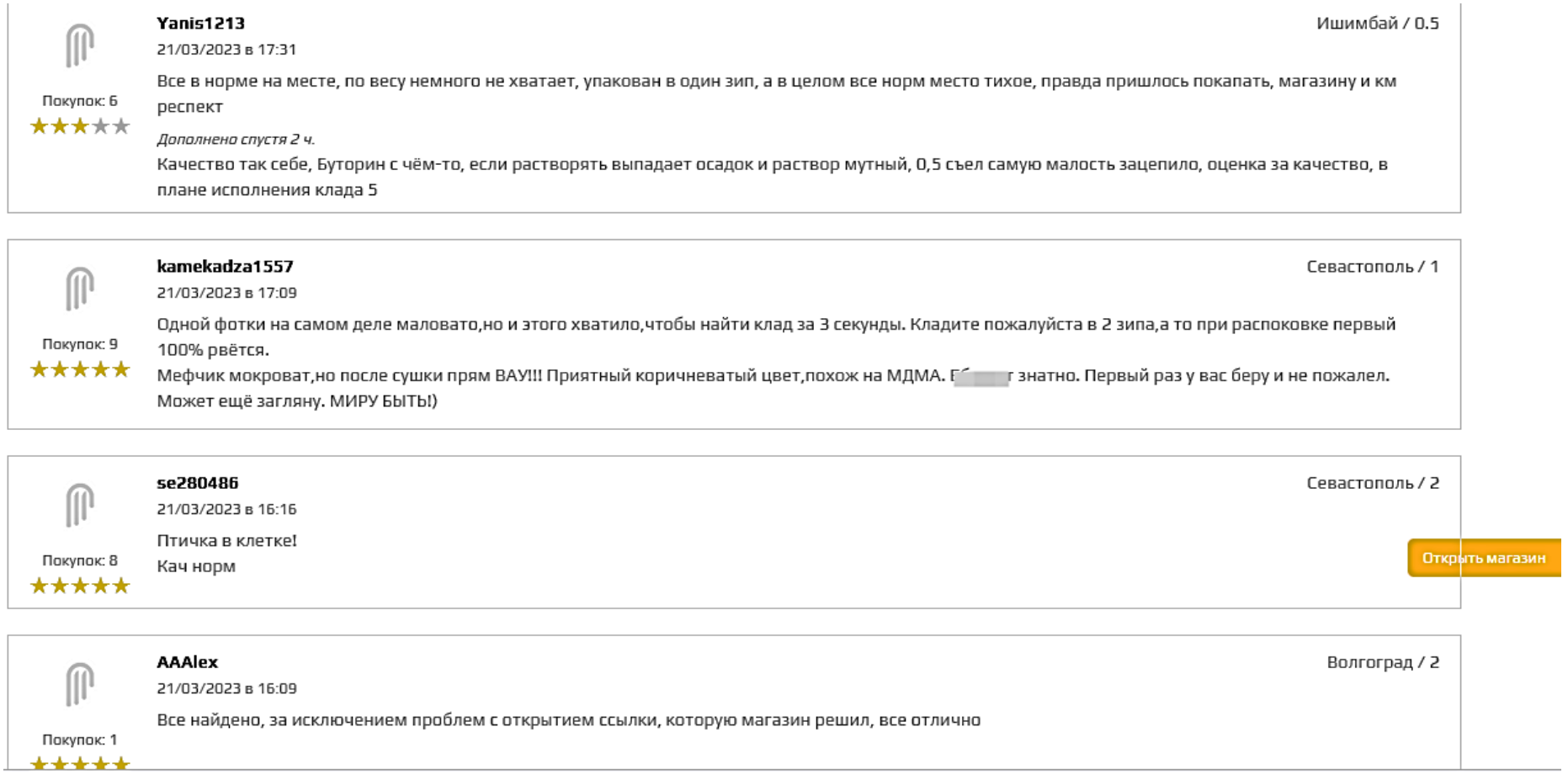

Рис. 4. *Отзывы потребителей наркотических средств*

Рис. 5. *Витрина магазина по продаже поддельных денежных купюр*

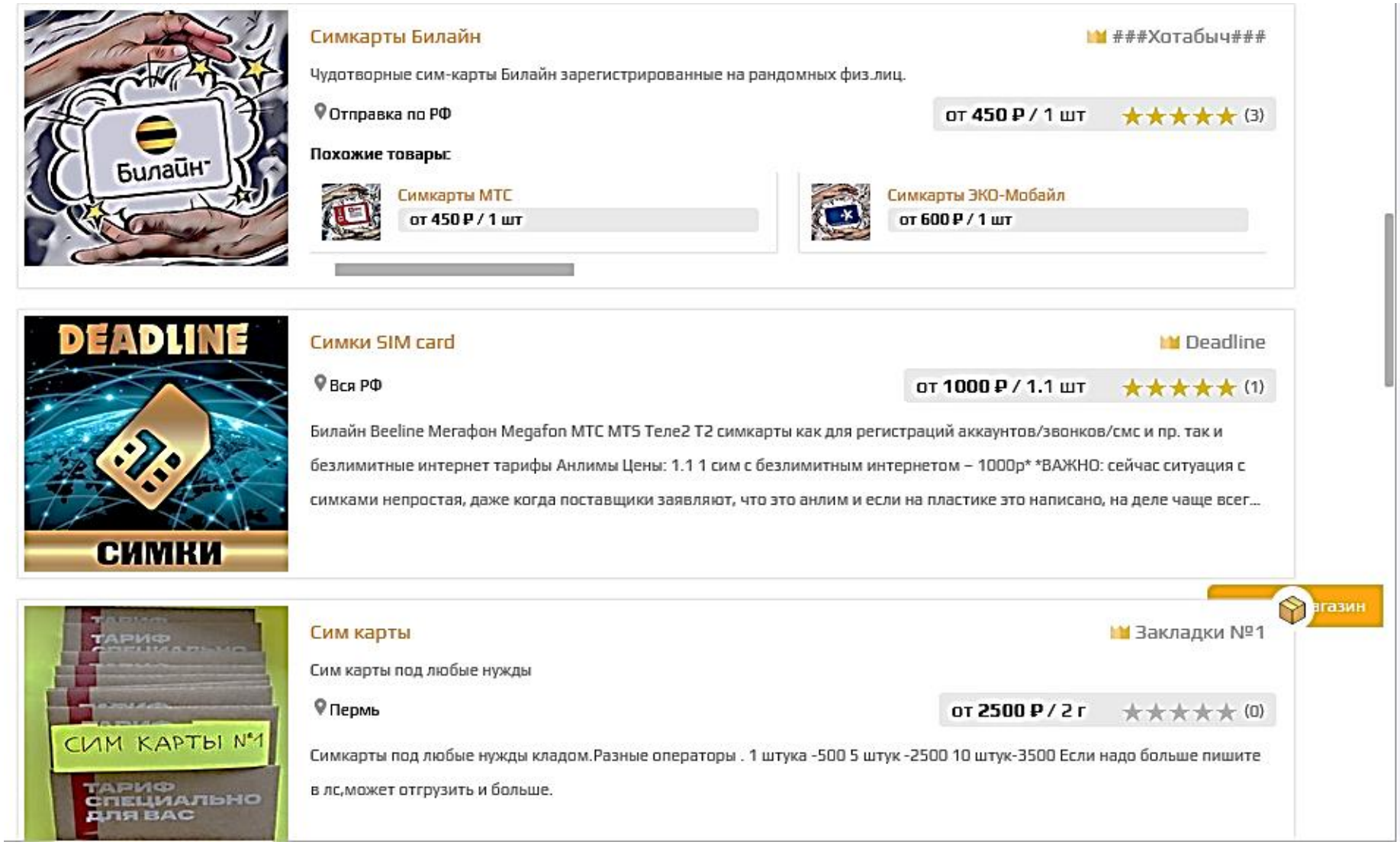

Рис. 6. *Магазины по продаже сим-карт*

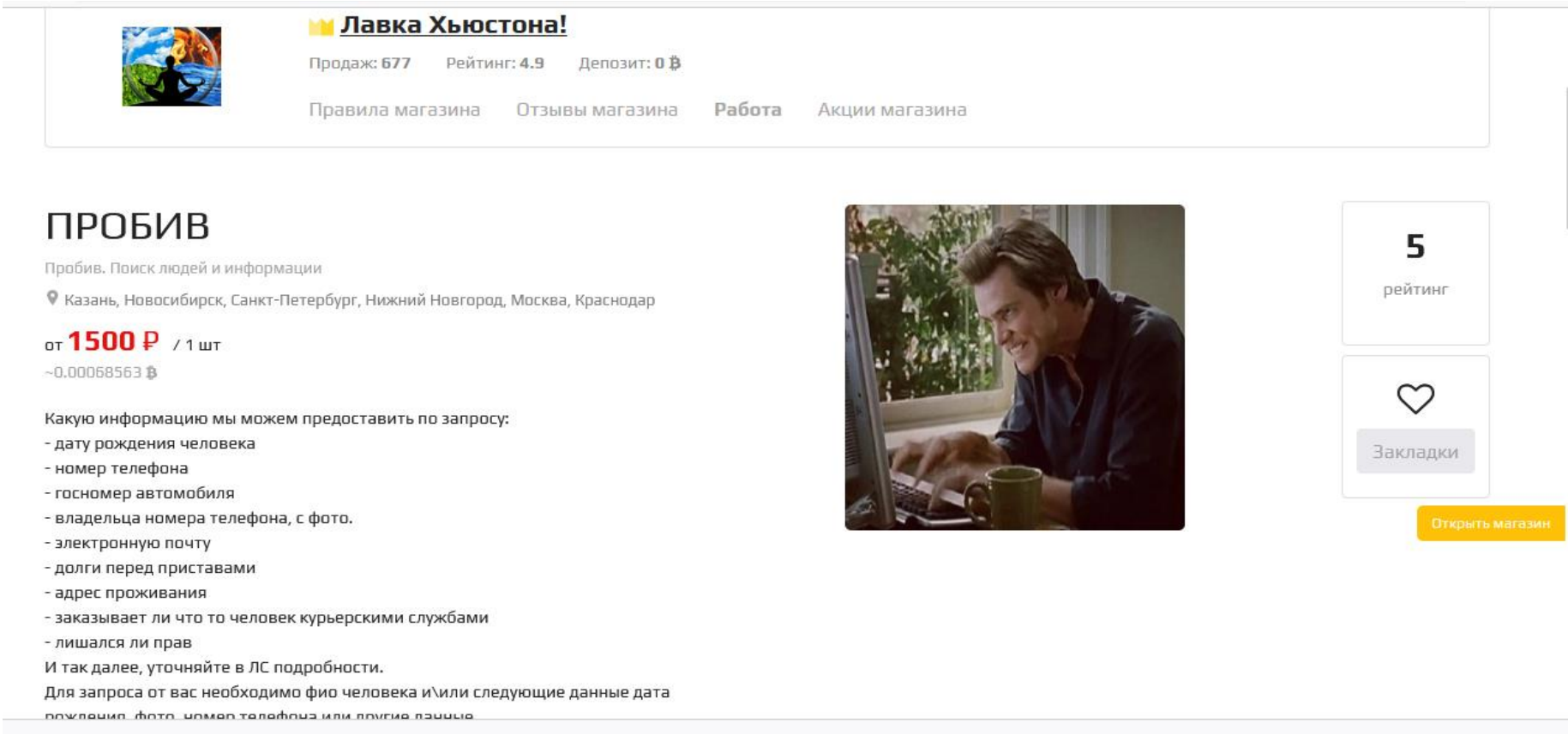

Рис. 7. *Витрина магазина, оказывающего услуги по предоставлению информации*

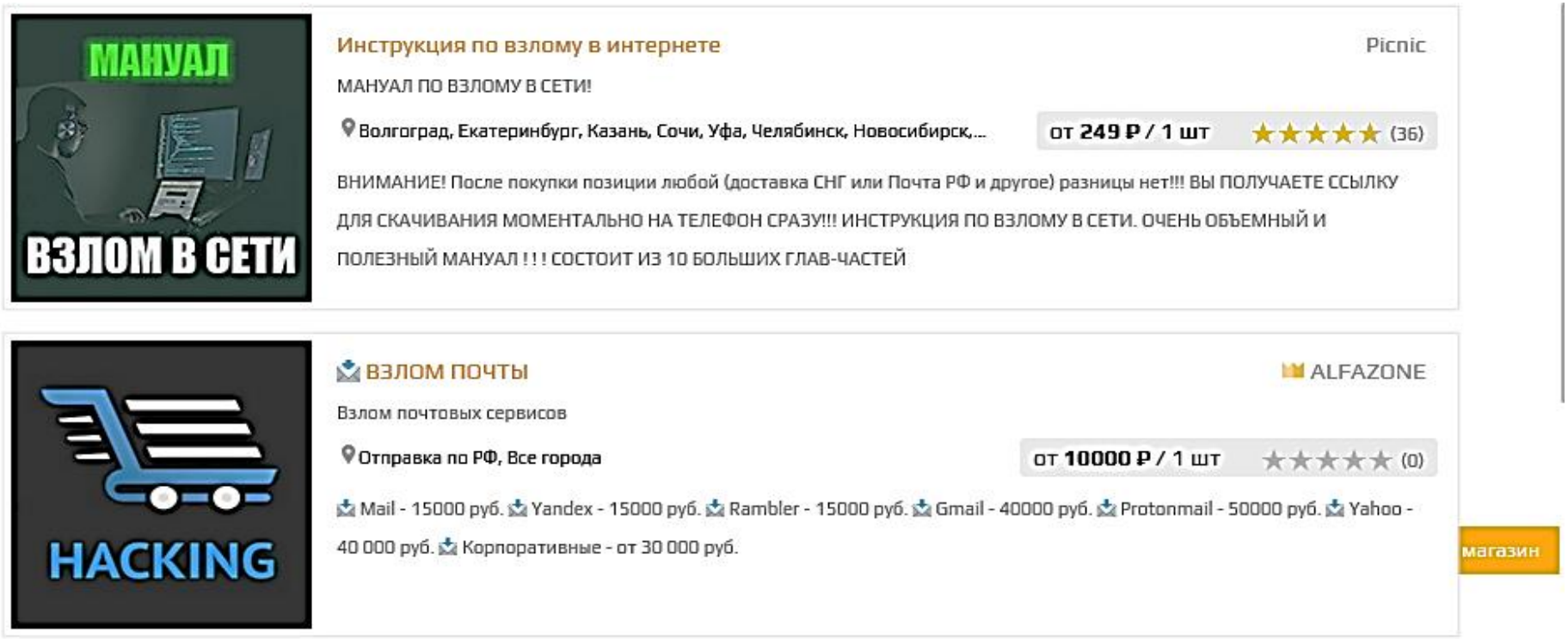

Рис. 8. *Магазины, оказывающие услуги по неправомерному доступу к компьютерной информации*

Эвакуация из РФ

THE BLACKCHAIN

Москва

от **500000 ₽** / 1 шт ★★★★★ (0)

Оказываем услуги по эвакуации из РФ, в т.ч. лицам в розыске. Помогаем обустроиться на новом месте. Цена - от 6000 у.е.

Все подробности - в ЛС.

Помощь с мобилизацией

LAB4U

Помогаем пересечь границу

Москва

от **1000 ₽** / 1 шт ★★★★★ (0)

Предлагаем официально отсрочку от мобилизации. Так же помощь пересечении границы Казахстана и получение официально гражданства Казахстана.

Рис. 9. *Магазины, оказывающие услуги по выезду за пределы Российской Федерации*

Приложение 2

Перечень нормативных правовых актов, относящих сведения к категории ограниченного доступа

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
Государственная тайна	Статья 5 Закона Российской Федерации от 21.07.1993 № 5485-1 «О государственной тайне»
	Указ Президента Российской Федерации от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»
	Статьи 5, 9 Федерального закона от 09.02.2007 № 16-ФЗ «О транспортной безопасности»
Коммерческая тайна	Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»
	Статья 12 Федерального закона от 28.11.2011 № 335-ФЗ «Об инвестиционном товариществе»
Персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных))	Статья 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
Налоговая тайна	Статьи 102, 313 Налогового кодекса Российской Федерации
Банковская тайна	Статья 857 Гражданского кодекса Российской Федерации (часть вторая)
	Статья 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»
	Статья 57 Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»
Врачебная тайна	Статьи 13, 92 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»
	Статья 15 Семейного кодекса Российской Федерации
	Статья 9 Закона Российской Федерации от 02.07.1992 № 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании»

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
	Статья 14 Закона Российской Федерации от 22.12.1992 № 4180-1 «О трансплантации органов и (или) тканей человека»
	Статья 13 Закона Российской Федерации от 20.07.2012 № 125-ФЗ «О донорстве крови и ее компонентов»
Нотариальная тайна	Статьи 16 и 28 Основ законодательства Российской Федерации о нотариате от 11.02.1993 № 4462-1
	Статья 26 Федерального закона от 05.07.2010 № 154-ФЗ «Консульский устав Российской Федерации»
Адвокатская тайна	Статья 8 Федерального закона от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»
Аудиторская тайна	Статья 9 Федерального закона от 30.12.2008 № 307-ФЗ «Об аудиторской деятельности»
Тайна страхования	Статья 946 Гражданского кодекса Российской Федерации (часть вторая)
	Статья 47 Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»
	Статья 18.2 Федерального закона от 24.07.1998 № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»
Тайна ломбарда	Статья 3 Федерального закона от 19.07.2007 № 196-ФЗ «О ломбардах»
Тайна связи	Статья 23 Конституции Российской Федерации
	Статьи 53 и 63 Федерального закона от 07.07.2003 № 126-ФЗ «О связи»
	Статья 15 Федерального закона от 17.07.1999 № 176-ФЗ «О почтовой связи»
Тайна завещания	Статья 1123 Гражданского кодекса Российской Федерации (часть третья)
Тайна усыновления	Статья 139 Семейного кодекса Российской Федерации

Сведения, отнесенные к категории ограниченного доступа	**Основания отнесения сведений к категории ограниченного доступа**
Тайна следствия	Статья 161 Уголовно-процессуального кодекса Российской Федерации
	Статья 20 Федерального закона от 10.06.2008 № 76-ФЗ «Об общественном контроле за обеспечением прав человека в местах принудительного содержания и о содействии лицам, находящимся в местах принудительного содержания»
Тайна судопроизводства	Статья 194 Гражданского процессуального кодекса Российской Федерации
	Статья 20 Арбитражного процессуального кодекса Российской Федерации
	Статьи 298 и 341 Уголовно-процессуального кодекса Российской Федерации
	Статья 175 Кодекса административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ
Конфиденциальность арбитража (третейского разбирательства)	Статья 21 Федерального закона от 29.12.2015 № 382-ФЗ «Об арбитраже (третейском разбирательстве) в Российской Федерации»
Отдельные сведения при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд	Статьи 24.1, 66, 68 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»
Сведения и предложения, содержащиеся в представленных заявках на участие в торгах при продаже предприятия-должника, или предложения о цене предприятия до начала торгов либо до момента открытия доступа к представленным в форме электронных документов заявкам на участие в торгах	Статья 110 Федерального закона от 26.10.2002 № 127-ФЗ «О несостоятельности (банкротстве)»
Сведения, представленные в электронной форме для проведения собрания кредиторов в случае банкротства гражданина	Статья 213.8 Федерального закона от 29.06.2015 № 154-ФЗ «Об урегулировании особенностей несостоятельности (банкротства) на территориях Республики Крым и города федерального значения Севастополя и о внесении изменений в отдельные законодательные акты Российской Федерации»

Сведения, отнесенные к категории ограниченного доступа	**Основания отнесения сведений к категории ограниченного доступа**
Сведения, ставшие известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния	Статья 13.2 Федерального закона от 15.11.1997 № 143-ФЗ «Об актах гражданского состояния»
Сведения о защищаемых лицах	Статья 9 Федерального закона от 20.08.2004 № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»
	Статья 9 Федерального закона от 20.04.1995 № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»
Сведения, ставшие известными гражданам в ходе оперативно-розыскной деятельности	Статья 17 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»
Сведения, содержащиеся в личном деле и документах учета сотрудника органов внутренних дел, в реестре сотрудников органов внутренних дел, а также сведения о гражданах, поступающих на службу в органы внутренних дел	Статьи 39 и 40 Федерального закона от 30.11.2011 № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации»
Сведения о военнослужащих (сотрудниках) войск национальной гвардии и членах их семей	Статья 23 Федерального закона от 03.07.2016 № 226-ФЗ «О войсках национальной гвардии Российской Федерации»
Сведения, содержащиеся в личном деле и документах учета сотрудника федеральной противопожарной службы	Статья 39 Федерального закона от 23.05.2016 № 141-ФЗ «О службе в федеральной противопожарной службе Государственной противопожарной службы и внесении изменений в отдельные законодательные акты Российской Федерации»
Сведения, которые стали известны эксперту в связи с проведением экспертизы по административному делу	Статья 49 Кодекса административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ
Сведения о несовершеннолетних, ставшие известными органам и учреждениям системы профилактики безнадзорности и правонарушений несовершеннолетних	Статья 9 Федерального закона от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»

Сведения, отнесенные к категории ограниченного доступа	**Основания отнесения сведений к категории ограниченного доступа**
Сведения о доходах, об имуществе и обязательствах имущественного характера, представляемые государственными и муниципальными служащими, а также иными лицами, указанными в части 1 статьи 8 Федерального закона от 25.12.2008 № 273-ФЗ	Статья 8 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции»
	Статья 20 Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации»
	Статья 15 Федерального закона от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации»
Сведения о расходах по приобретению земельного участка, другого объекта недвижимости, транспортного средства, ценных бумаг, акций (долей участия, паев в уставных (складочных) капиталах организаций) и об источниках получения средств, за счет которых совершена сделка, представляемые лицами, замещающими (занимающими) одну из должностей, указанных в пункте 1 части 1 статьи 2 Федерального закона от 03.12.2012 № 230-ФЗ	Статья 8 Федерального закона от 03.12.2012 № 230-ФЗ «О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам»
Информация, относящаяся к процедуре медиации	Статья 5 Федерального закона от 27.07.2010 № 193-ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)»
Конфиденциальность третейского разбирательства	Статья 22 Федерального закона от 24.07.2002 № 102-ФЗ «О третейских судах в Российской Федерации»
Информация о содержании корпоративного договора, заключенного участниками непубличного общества	Статья 67.2 Гражданского кодекса Российской Федерации (часть первая)
Информация о новых решениях и технических знаниях, полученных сторонами по договору подряда	Статья 727 Гражданского кодекса Российской Федерации (часть вторая)
Сведения, касающиеся предмета договоров на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, хода их исполнения и полученных результатов, если иное не предусмотрено договорами	Статья 771 Гражданского кодекса Российской Федерации (часть вторая)

Сведения, отнесенные к категории ограниченного доступа	**Основания отнесения сведений к категории ограниченного доступа**
Секрет производства (ноу-хау)	Статья 1465 Гражданского кодекса Российской Федерации (часть четвертая)
Информация о проектных решениях и иная конфиденциальная информация, которая стала известна органу исполнительной власти или организации, проводившим экспертизу проектной документации и (или) результатов инженерных изысканий в связи с проведением экспертизы	Статья 49 Градостроительного кодекса Российской Федерации
Информация, предоставляемая организациям (гражданам), осуществляющим производство и выпуск средств массовой информации	Статья 41 Закона Российской Федерации от 27.12.1991 № 2124-1 «О средствах массовой информации»
Информация, входящая в состав кредитной истории, и (или) код субъекта кредитной истории	Статьи 6 и 7 Федерального закона от 30.12.2004 № 218-ФЗ «О кредитных историях»
Сведения о должнике, просроченной задолженности и ее взыскании и любые другие персональные данные должника	Статья 6 Федерального закона от 03.07.2016 № 230-ФЗ «О защите прав и законных интересов физических лиц при осуществлении деятельности по возврату просроченной задолженности и о внесении изменений в Федеральный закон «О микрофинансовой деятельности и микрофинансовых организациях»
Кредитное рейтинговое агентство обязано соблюдать условия конфиденциальности информации, полученной от рейтингуемого лица, а также соблюдать требования к сохранности и защите информации, полученной в процессе деятельности кредитного рейтингового агентства, установленные Банком России	Статья 9 Федерального закона от 13.07.2015 № 222-ФЗ «О деятельности кредитных рейтинговых агентств в Российской Федерации, о внесении изменения в статью 76.1 Федерального закона «О Центральном банке Российской Федерации (Банке России)» и признании утратившими силу отдельных положений законодательных актов Российской Федерации»
Сведения, ставшие известными саморегулируемой организации, о финансовых организациях, являющихся членами саморегулируемой организации, финансовых организациях, представивших документы для приема в члены, в кандидаты в члены	Статья 13 Федеральный закон от 13.07.2015 № 223-ФЗ «О саморегулируемых организациях в сфере финансового рынка и о внесении изменений в статьи 2 и 6 Федерального закона “О внесении изменений в отдельные законодательные акты Российской Федерации”»

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
саморегулируемой организации, в том числе сведений об их клиентах	
Информация: – полученная в связи с осуществлением функций трансфер-агента; – полученная держателями реестра и депозитариями; – получаемая репозитарием на основании договора об оказании репозитарных услуг, а также целостность записей, составляющих реестр договоров; – предоставляемая Банку России	Статьи 8.1, 8.6, 15.8, 44.1 Федерального закона от 22.04.1996 № 39-ФЗ «О рынке ценных бумаг»
Информация о счетах и об операциях клиентов центрального депозитария	Статья 14 Федерального закона от 07.12.2011 № 414-ФЗ «О центральном депозитарии»
Информация, предоставляемая клиринговым организациям и лицам, осуществляющим функции центрального контрагента	Статья 20 Федерального закона от 07.02.2011 № 7-ФЗ «О клиринге и клиринговой деятельности»
Сведения, полученные в процессе проведения экспертизы моделей контрольно-кассовой техники и технических средств оператора фискальных данных. Конфиденциальность фискальных данных, мастер-ключей и ключей фискального признака	Статьи 3.1, 4.1, 4.5 Федерального закона от 22.05.2003 № 54-ФЗ «О применении контрольно-кассовой техники при осуществлении наличных денежных расчетов и (или) расчетов с использованием электронных средств платежа»
Факт передачи в федеральный орган исполнительной власти, принимающий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма информации, указанной в пунктах 1–3 статьи 7.1-1 Федерального закона от 07.08.2001 № 115-ФЗ	Статья 7.1-1 Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»
Инсайдерская информация	Статья 6 Федерального закона от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»
Сведения, предоставляемые	Статья 23 Федерального закона от 21.11.2011

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
участниками торгов в соответствии с правилами организованных торгов	№ 325-ФЗ «Об организованных торгах»
Информация, полученная в связи с осуществлением деятельности по выдаче, погашению и обмену инвестиционных паев	Статья 28 Федерального закона от 29.11.2001 № 156-ФЗ «Об инвестиционных фондах»
Информация, полученная в ходе проведения проверок российских участников внешнеэкономической деятельности	Статья 17 Федерального закона от 18.07.1999 № 183-ФЗ «Об экспортном контроле»
Сведения о результатах проведенной оценки уязвимости объектов транспортной инфраструктуры и транспортных средств, сведения, содержащиеся в планах обеспечения транспортной безопасности объектов транспортной инфраструктуры и транспортных средств, информационные ресурсы единой государственной информационной системы обеспечения транспортной безопасности	Статьи 5, 9, 11 Федерального закона от 09.02.2007 № 16-ФЗ «О транспортной безопасности»
Сведения, составляющие дактилоскопическую информацию	Статья 12 Федерального закона от 25.07.1998 № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации»
Информация, содержащаяся в контрольных измерительных материалах, используемых при проведении государственной итоговой аттестации	Статья 59 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»
Сведения о платежах в соответствующие бюджеты бюджетной системы Российской Федерации и об их плательщиках, поступающие в финансовые органы от органов Федерального казначейства	Статья 241 Бюджетного кодекса Российской Федерации
Сведения, содержащиеся в индивидуальных лицевых счетах застрахованных лиц в системе обязательного пенсионного страхования	Статья 6 Федерального закона от 01.04.1996 № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»
Информация, полученная НПФ при обработке сведений, содержащихся в пенсионных счетах	Статья 15 Федерального закона от 07.05.1998 № 75-ФЗ «О негосударственных пенсионных фондах»

Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
негосударственного пенсионного обеспечения, пенсионных счетах накопительной части трудовой пенсии и др.	
Информация о получателе социальных услуг	Статья 6 Федерального закона от 28.12.2013 № 442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации»
Сведения, содержащиеся в Федеральной государственной информационной системе учета результатов проведения специальной оценки условий труда	Статья 18 Федерального закона от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда»
Сведения, ставшие известными судебным приставам в связи с исполнением должностных обязанностей	Статья 4 Федерального закона от 21.07.1997 № 118-ФЗ «О судебных приставах»
Информация, представляемая заинтересованным лицом в орган, проводящий расследования в целях принятия решения о целесообразности введения, применения, пересмотра или отмены специальной защитной меры, антидемпинговой меры или компенсационной меры	Статья 32 Федерального закона от 08.12.2003 № 165-ФЗ «О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров»
Информация о членах политической партии, представляемая для сведения в уполномоченные органы	Статья 19 Федерального закона от 11.07.2001 № 95-ФЗ «О политических партиях»
Тайна исповеди	Статья 3 Федерального закона от 26.09.1997 № 125-ФЗ «О свободе совести и о религиозных объединениях»
Сведения о населении, содержащиеся в переписных листах	Статья 8 Федерального закона от 25.01.2002 № 8-ФЗ «О Всероссийской переписи населения»
Сведения, содержащиеся в переписных листах об объектах сельскохозяйственной переписи	Статья 12 Федерального закона от 21.07.2005 № 108-ФЗ О Всероссийской сельскохозяйственной переписи»
Первичные статистические данные, содержащиеся в формах федерального статистического наблюдения	Статья 9 Федерального закона от 29.11.2007 № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации»

Сведения, отнесенные к категории ограниченного доступа	**Основания отнесения сведений к категории ограниченного доступа**
Информация, содержащаяся в паспортах безопасности объектов топливно-энергетического комплекса	Статья 8 Федерального закона от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»
Информация, полученная членами саморегулируемой организации в области энергетического обследования в ходе проведения энергетического обследования	Статья 18 Федерального закона от 23.11.2009 № 261-ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации»
Сведения, содержащиеся в заявках на участие в конкурсе на право заключить контракт на проведение лотерей	Статья 24.10 Федеральный закон от 11.11.2003 № 138-ФЗ «О лотереях»
Сведения, ставшие известными уполномоченному по правам человека в субъекте Российской Федерации в процессе рассмотрения жалобы о частной жизни лица, подавшего жалобу, и других лиц без их письменного согласия	Статья 16.1 Федерального закона от 06.10.1999 № 184-ФЗ «Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации»
Запрещается опубликование (обнародование) в день голосования до момента окончания голосования на территории Российской Федерации данных об итогах голосования, о результатах выборов Президента РФ, в том числе размещение таких данных в информационно-телекоммуникационных сетях, доступ к которым не ограничен определенным кругом лиц (включая сеть «Интернет»)	Статья 46 Федерального закона от 10.01.2003 № 19-ФЗ «О выборах Президента Российской Федерации»
Информация, полученная при осуществлении своих полномочий службой внутреннего аудита публично-правовой компании	Статья 16 Федерального закона от 03.07.2016 № 236-ФЗ «О публично-правовых компаниях в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»
Информация, содержащаяся в профилях и индикаторах рисков, применяемых таможенными органами	Статья 315 Федеральный закон от 03.08.2018 № 289-ФЗ «О таможенном регулировании в Российской Федерации и о внесении изменений в отдельные законодательные акты Российской Федерации»

Приложение 3

Образец запроса

Генеральному
директору
ООО «ВКонтакте»

ЗАПРОС

В связи с расследованием уголовного дела №_____, возбужденного *дд.мм.гггг* по признакам преступления, предусмотренного ст. _____ УК РФ, на основании ч. 4 ст. 21 УПК РФ прошу Вас предоставить следующую информацию в отношении пользователя, осуществлявшего подключение к учетной записи «Иван Петров» (id275949102) с *дд.мм.гггг* (*дата неправомерного доступа к учетной записи)* по *дд.мм.гггг* (*дата восстановления доступа легитимным пользователем или дата блокировки учетной записи администрацией веб-сайта)*:

– сведения об IP-адресах, с которых осуществлялось подключение к учетной записи;

– сведения, характеризующие программно-аппаратные средства пользователя, осуществляющего подключение к учетной записи (user-agent, canvas, time zone и другие отпечатки веб-браузера (browser fingerprints));

– сведения об иных IP-адресах и иных связанных с пользователем учетных записях, подключение к которым происходило при использовании одного веб-браузера, полученные посредством анализа cookie-файлов и отпечатков браузера (browser fingerprints).

Следователь ФИО / Подпись

Учебное издание

кандидат юридических наук
Поздышев Роман Сергеевич;
кандидат юридических наук, доцент
Саакян Артём Григорьевич;
кандидат юридических наук, доцент
Долгачёва Оксана Игоревна
(Нижегородская академия МВД России);
Васильев Алексей Евгеньевич
(Следственный департамент МВД России);
кандидат юридических наук, доцент
Николаева Татьяна Анатольевна
(Приволжский филиал
Российского государственного университета правосудия);

РАССЛЕДОВАНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНЫХ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Учебное пособие

Редактор *Т. Ю. Булганина*
Компьютерная верстка *Т. В. Булкиной*
Дизайн обложки *К. А. Быкова*

Подписано в печать 21.12.2023. Формат 60x84/16. Усл. печ. л. 4,47
Тираж 100 экз. Заказ 424

Редакционно-издательский отдел
Нижегородской академии МВД России

Отпечатано в отделении полиграфической и оперативной печати
Нижегородской академии МВД России

603144, Н. Новгород, Анкудиновское шоссе, 3