УГОЛОВНО-ПРАВОВЫЕ НАУКИ

Научная статья
УДК 343.985.2
DOI: 10.55001/2587-9820.2024.40.14.001

СОВРЕМЕННЫЕ ПОДХОДЫ И ВОЗМОЖНОСТИ ДЛЯ ПОЛУЧЕНИЯ И АНАЛИЗА ЦИФРОВЫХ ДАННЫХ ПРИ ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

Ахмед Мухамедович Арипшев[1], Руслан Хазраилович Шондиров[2]
[1,2]Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России, г. Нальчик, Российская Федерация,
[1]aripshev@yandex.ru
[2]rshondirov@mail.ru

Аннотация. Авторы статьи исследуют современные подходы и возможности сотрудников оперативных подразделений органов внутренних дел для получения и анализа цифровых данных при противодействии киберпреступности. Пристальное внимание в настоящем исследовании обращено на организационно-тактические и технические методы получения оперативно-розыскной информации для использования в раскрытии преступлений, совершаемых с использованием современных технических средств и сетей передачи данных. Также в статье рассматривается технический аспект получения оперативно значимой информации: о личности пользователя интернет-ресурсов; установлении владельцев веб-сайтов, отправителей электронных сообщений, владельцев электронных кошельков, а также других сведений, имеющих значение для раскрытия интернет-преступлений.

Ключевые слова: оперативно-розыскная деятельность, оперативно-розыскные мероприятия, цифровые данные, сбор оперативно значимой информации, сеть Интернет, интернет-сервисы, деанонимизация

Для цитирования: Арипшев, А. М., Шондиров, Р. Х. Современные подходы и возможности для получения и анализа цифровых данных при противодействии киберпреступности // Криминалистика: вчера, сегодня, завтра : сб. науч. тр. Иркутск : Восточно-Сибирский институт МВД России. 2024. Т. 32. № 4. С. 7–15. DOI: 10.55001/2587-9820.2024.40.14.001

MODERN APPROACHES AND POSSIBILITIES FOR OBTAINING AND ANALYZING DIGITAL DATA IN COUNTERING CYBERCRIME

Akhmed M. Aripshev[1], Ruslan Kh. Shondirov[2]
[1,2]North Caucasus Institute for Advanced Studies (branch) of Krasnodar University of the MIA of Russia, Nalchik, Russian Federation
[1]aripshev@yandex.ru
[2]rshondirov@mail.ru

Abstract. The authors of the article examine modern approaches and capabilities of the employees of operational units of the internal affairs bodies to obtain and analyze digital data when combating cybercrime. In this study, close attention is paid to the organizational, tactical and technical methods of obtaining operational-search information for use in solving crimes committed using modern technical means and data transmission networks. Another issue of the article was the technical aspect of obtaining operationally significant information: about the identity of the user of Internet resources; establishing the owner of websites; senders of electronic messages; owners of electronic wallets and other effective

methods of obtaining information, including searching the Internet, using specialized services and software that can be used to solve the problems assigned by the Federal Law "On Operational-Investigative Activities" to the subjects of operational-investigative activities.

Keywords: Operational investigative activities, operational investigative measures, digital data, collection of operationally significant information, Internet, Internet services, deanonymization

For citation: Aripshev A. M., Shondirov R. Kh. Sovremennye podhody i vozmozhnosti dlya polucheniya i analiza cifrovyh dannyh pri protivodejstvii kiberprestupnosti [Modern approaches and possibilities for obtaining and analyzing digital data in countering cybercrime]. Kriminalistika: vchera segodnya, zavtra = Forensics: yesterday, today, tomorrow. 2024, vol. 32, no 4, pp. 7–15 (in Russ.) DOI: 10.55001/2587-9820.2024.40.14.001

Введение

Сегодня сеть Интернет стала неотъемлемой частью повседневной жизни, предоставляя огромное количество информации и возможностей. Социальные сети, онлайн-ресурсы, интернет-магазины и информационные сайты создают огромное пространство, которое предоставляет широкие возможности, в том числе для преступников. Преступность в онлайн-пространстве возникла с самого начала существования Интернета и продолжает совершенствоваться.

Ежегодно появляются новые методы и формы совершения преступлений. Причины распространения IT-преступности довольно просты: в сети гораздо сложнее выявить факт совершения преступления, практически нет возможности его предотвратить, а расследование таких деяний осложняется анонимностью преступников, отсутствием свидетелей и улик. «При этом приходится констатировать, что тенденция повышения уровня сетевой преступности среди населения, особенно молодежного возраста, имеет тенденцию к росту, что требует от оперативных подразделений ОВД внедрения и использования эффективных методов и средств борьбы с киберпреступностью» [1, с. 109].

Эффективность борьбы оперативных подразделений органов внутренних дел (далее – ОВД) с IT-преступностью во многом зависит от организационно-тактической готовности. К ней относятся вопросы планирования, координации и контроля действий оперативных служб, а также выбора наиболее эффективных методов и приемов работы. Технические аспекты включают в себя использование специальных программ и инструментов для поиска, анализа и обработки информации, а также обеспечение безопасности и конфиденциальности данных.

Мы согласны с С. В. Тимофеевым, что «современные технологии позволяют преступникам, находясь в одном месте, совершать противоправные действия в отношении лиц, проживающих в другом регионе или даже в другой стране. Поэтому, желая сохранить в государстве правопорядок и обезопасить граждан от преступных посягательств, сотрудники правоохранительных органов, различных силовых ведомств и специальных служб мира постоянно совершенствуют средства противодействия киберпреступности путем разработки, внедрения и использования в ОРД специальных программ слежения за действиями в сети Интернет лиц, представляющих оперативный интерес» [2, с. 133].

О. П. Грибунов, П. В. Никонов и С. В. Пархоменко указывали, что «активное внедрение цифровых технологий в различные сферы жизни

общества требует в том числе разработки адекватного нормативного правового регулирования новых общественных отношений и создания правовых гарантий цифровой безопасности» [3, с. 6].

В научной литературе сравнительно мало работ по проблемам добывания оперативно-значимой информации с использованием ресурсов сети Интернет. Поэтому цель данной статьи состоит в исследовании теоретических и практических аспектов получения оперативно-значимой информации с использованием ресурсов сети Интернет.

Основная часть

При раскрытии преступлений, совершенных в сети Интернет, основной проблемой как в организационном, тактическом, техническом, так и правовом аспектах является проблема деанонимизации личности пользователя ресурсов сети Интернет, определения местоположения абонентского устройства или средства обеспечения связи [4, с. 171]. В данном случае особое значение приобретает знание технических особенностей электронных устройств, к числу которых следует отнести следующие идентификаторы:

– IMSI – международный идентификатор абонента сети подвижной связи;

– IMEI – международный идентификатор мобильного оборудования;

– MAC-адрес – уникальный идентификатор оборудования сетей передачи данных;

– ICQ – идентификатор служб обмена сообщениями;

– MIN – мобильный идентификационный номер мобильной абонентской радиостанции;

– IP-адрес – уникальный сетевой адрес компьютера в сети, построенный по протоколу IP, где под уникальностью IP-адреса понимается использование конкретного IP-адреса в сети в определенное время одним устройством.

В соответствии с предметом нашего исследования особое внимание обратим на особенности IP-адреса, который имеет следующие виды:

– приватные «серые» IP-адреса;

– коллективные IP-адреса;

– сетевые IP-адреса;

– не выделенные или не присвоенные регистратором IP-адреса.

При этом в практике деятельности оперативных подразделений выделяются два вида IP-адресов: статический и динамический.

Статическим, постоянным и неизменяемым, IP-адресом называют адрес, назначенный пользователем в настройках устройства либо автоматически при подключении устройства к сети, который, соответственно, не может быть присвоен другому техническому устройству.

Динамическим, непостоянным и изменяемым, IP-адресом называют адрес, назначенный автоматически при подключении устройства к сети на определенный промежуток времени.

С учетом особенностей построения сети Интернет рассмотрим организационно-тактические аспекты подготовки и проведения оперативно-розыскных мероприятий (далее – ОРМ).

Регистрацией IP-адресов в сети Интернет занимаются регистраторы – «IP-registry». Данная система имеет трехуровневую иерархию, где «IANA» является основным регистратором, регистрирующим крупные блоки IP-адресов. «IANA» в свою очередь делится на так называемые регистраторы RIR, которых в настоящее время пять. RIR делятся на LIR – так называемые местные регистраторы, которые выделяют более мелкие диапазоны IP-адресов.

В настоящее время используются две формы записи IP-адреса: IPv4 и IPv6. IPv4 представляет собой запись четырех десятичных чисел значением от 0 до 255, разделенных точками. Например, размер адреса 192.168.0.1. составляет 32 бита. IPv6 является более современной версией протокола IP, где длина адреса составляет 128 бит.

На наш взгляд, при решении задач ОРД важно использовать регистрационные данные, полученные в том числе из общедоступных интернет-сервисов, например «WHOIS». Используя глобальные справочные интернет-сервисы, сотрудник оперативного подразделения ОВД может получить информацию о регистрационных данных владельцев IP-адресов и доменных имен, установить интернет-провайдера, которому принадлежит IP-адрес.

При этом важно отметить, что использование глобальных сервисов неэффективно для следующих диапазонов IP-адресов:

– 10.0.0.1–10.255.255.254;
– 127.0.0.1–127.255.255.254;
– 169.254.0.1–169.254.255.254;
– 172.16.0.1–172.31.255.254;
– 192.168.0.1–192.168.255.254.

Это обусловлено тем, что указанные диапазоны используются для адресации внутри локальных и частных сетей передачи данных в так называемых «серых» IP-адресах. Подключение указанных IP-адресов к сети Интернет осуществляется с использованием общего NAT-сервера, где, как правило, с использованием такого IP-адреса к сети подключается одновременно несколько тысяч абонентов.

При установлении интернет-провайдера или оператора сети с целью получения оперативно значимой информации сотруднику оперативного подразделения необходимо направить в рамках ОРМ «Наведение справок» запрос оператору связи о предоставлении данных пользователя.

В запросе, как правило, отражается, является ли интересующий IP-адрес динамическим или статическим; выделен ли он NAT-серверу или оконечному пользователю. Кроме того, при наведении справок необходимо указывать конкретный IP-адрес и период времени его подключения. В случае отсутствия IP-адреса источника имеется техническая возможность установления его с помощью интернет-сервиса «WHOIS», для чего необходимо указать вместо IP-адреса доменное имя источника.

Нередко в целях решения задач ОРД возникает необходимость установления отправителя электронного письма. Каждое электронное письмо содержит информацию о маршруте следования в процессе отправки–получения – RFC-заголовок. При этом, как правило, по умолчанию данная информация у получателя не отображается. Анализ информации о движении электронного письма позволяет получить сведения об IP-адресе компьютера, с которого письмо было отправлено, а также информацию об электронном почтовом ящике. В некоторых случаях при получении письма целенаправленно может быть указан произвольный либо не принадлежащий интересующему оперативного сотрудника лицу электронный почтовый ящик.

Для установления IP-адреса устройства, с которого было отправлено письмо, необходимо открыть электронное письмо и в командной панели выбрать «отображение свойств письма», в зависимости от используемого почтового клиента. Как правило, IP-адрес отправителя содержится в полях «X-Originating-IP» или «Received: from».

Далее необходимо обратить внимание на последний отображенный IP-адрес. Дата и время отправления письма указаны в поле «Date» или «Received from», где значение +0300 указывает на часовой пояс относительно нулевого меридиана.

Если полученный IP-адрес принадлежит диапазонам 10.0.0.1–10.255.255.254, 127.0.0.1–127.255.255.254, 169.254.0.1–169.254.255.254, 172.16.0.1–192.168.255.254, то необходимо выбрать IP-адрес, расположенный выше отображенного – соответственно, полученный IP-адрес использовать для идентификации абонента во внутренней сети определенного интернет-провайдера. Уже после этого возможно установить регистрационные данные по IP-адресу.

Важное значение для ОРД имеет и установление владельца электронного почтового ящика (e-mail). В современных условиях практически каждый человек в своей повседневной деятельности использует так называемый электронный почтовый ящик, который содержит ценную и важную информацию о его владельце. В целях установления принадлежности электронного почтового ящика конкретному пользователю необходимо осуществить ряд мероприятий.

Для начала необходимо установить принадлежность почтового ящика сервису электронной почты. Адрес электронной почты состоит из имени пользователя и доменного имени, которые разделяются знаком @. Доменное имя – это адрес сайта, на котором зарегистрирован почтовый ящик. Приведем список наиболее распространенных электронных почтовых ящиков:

- ООО «Мэйл.Ру» – @mail.ru, @inbox.ru, @list.ru, @bk.ru;
- ООО «Яндекс» – @yandex.ru;
- ООО «Рамблер Интернет Холдинг» – @rambler.ru, @lenta.ru, @autorambler.ru, @ro.ru.

Почтовые ящики @gmail.com, @botmail.com, @yahoo.com принадлежит сервисам электронной почты, находящимся в США. В связи с тем, что Российская Федерация не ратифицировала Конвенцию Совета Европы о киберпреступности[1], компания Google отклоняет запросы российских правоохранительных органов о данных пользователей [5, с. 129].

Оперативный сотрудник с целью установления регистрационных данных пользователя почтового ящика должен направить в рамках ОРМ «Наведение справок» запрос о предоставлении активности электронного почтового ящика. Перед тем как направить запрос, следует проверить наличие почтового ящика, для чего необходимо попытаться восстановить пароль данного почтового ящика. В запросе должна быть отражена информация о регистрационных данных, IP-адресах авторизации, абонентском номере активации и т. д. Соответственно, в ответе на запрос должна содержаться информация об IP-адресах, с которых владелец осуществлял те или иные действия в электронной почте. После получения IP-адреса сотрудник имеет возможность определить установочные данные лица и получить сведения о его физическом местоположении.

Еще больший интерес с точки зрения добывания оперативно значимой информации представляет установление владельца интернет-сайта.

Интернет-сайт или веб-сайт (от англ. website: web – «паутина, сеть», site – «место») – это совокупность электронных документов физического лица или организации в компьютерной сети, объединенных одним адресом, где доменное имя – это символьное имя, служащее для идентификации сетевых ресурсов.

Доменные имена предоставляют возможность адресации компьютеров и расположенных на них сетевых ресурсов. Соответственно, хостинг-провайдер – это компания, занимающаяся предоставлением услуг по размещению интернет-сайтов на своих технологических площадках.

Для установления владельца вебсайта также необходимо использовать интернет-сервис «WHOIS-сервис», предоставляющий информацию о регистрационных данных владельцев IP-адресов, доменных адресов. После необходимо получить открытую информацию о регистраторе доменного имени и организации, на ресурсах которой размещен интернет-сайт с интересующим доменным именем.

Более подробно рассмотрим данную процедуру на примере доменного имени URL: https:www.consultant.ru.

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // Гарант : сайт. URL: https://base.garant.ru/4089723/?ysclid=ls1q0f9i531877814 (дата обращения: 30.01.2024).

В качестве владельца имени указана организация «Joint-Stock Company Consultant Plus». В данном случае информация соответствует действительности, но нередки случаи, когда в графе «владелец» указано частное лицо – «Private person» (рис. 1).

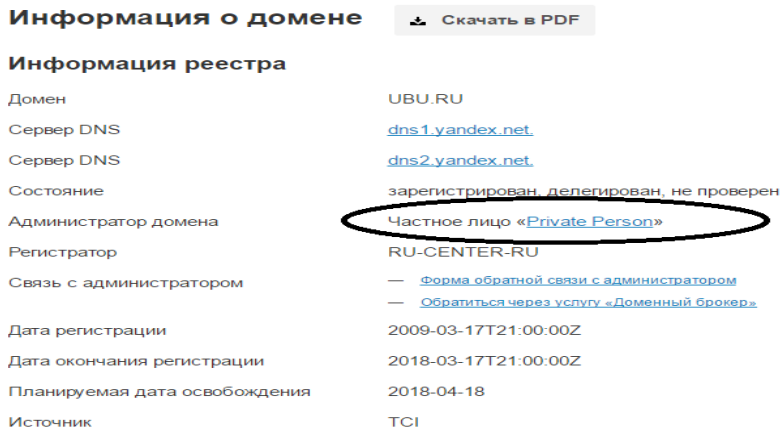

Рис. 1. Информация из реестра о домене

В таких случаях сотруднику оперативного подразделения ОВД необходимо направлять в рамках ОРМ «Наведение справок» запрос в компанию регистратора домена – в нашем случае это компания «RU-CENTER-RU». Зачастую владелец домена предоставляет информацию, не соответствующую действительности. В полученной информации в поле «Регистратор» указан владелец хостинга (в нашем случае это «RU-CENTER-RU»), который может предоставить регистрационные данные, а также IP-адреса авторизации, контактные данные, платежные реквизиты, которые являются достоверными.

Важное значение имеет и установление пользователя социальной сети, под которой понимается интернет-ресурс, предназначенный для обмена различного рода информацией.

Социальная сеть содержит необходимую цифровую информацию для решения задач ОРД, в том числе и деанонимизирующей пользователя сети Интернет [6, с. 171].

Пользователи в социальной сети идентифицируются по уникальным номерам (ID) либо по электронному почтовому ящику. С целью установления пользователя социальной сети сотруднику оперативного подразделения ОВД необходимо определить уникальный идентификатор пользователя – ID.

Сведения об ID указаны в адресной строке браузера после текста «vk.com/». ID состоит из последовательности цифр или латинских букв. Сотруднику оперативного подразделения ОВД с целью установления регистрационных данных пользователя социальной сети следует направить в рамках ОРМ «Наведение справок» запрос в организацию, владеющую социальной сетью. В обращении следует запросить информацию о регистрационных данных пользователя, информацию об IP-адресах и времени авторизации, контактные телефоны, номера электронных кошельков, с которых производилась оплата услуг и т. д. [7, с. 171].

Особое внимание следует обратить на установление владельца электронного кошелька, т. е. интернет-сервиса, предназначенного для пополнения, хранения, перечисления электронных денег, оплаты различных услуг, обмена электронных денег на реальные.

Е. И. Третьякова справедливо отметила, что «электронная система

расчетов становится в центре финансового обращения. Свое преимущество она очередной раз доказала в период возникшей в мире пандемии коронавирусной инфекции COVID-19. В период самоизоляции электронная система расчетов позволяла гражданам получать заработную плату, государственные выплаты, осуществлять различные платежи, приобретать товары через Интернет и осуществлять другие финансовые операции» [6, с. 196].

Для определения владельца электронного кошелька необходимо установить уникальный идентификатор кошелька в электронной платежной системе и направить соответствующий запрос.

Приведем список наиболее распространенных платежных систем, используемых в том числе в преступных целях.

1. «Webmoney» – электронный кошелек платежной системы ООО «Вебмани.Ру». Имеет вид R124315355363, где «R» – это рубли, «Z» – доллары США. Уникальный номер пользователя имеет, например, такой вид: WHJJ 14147128644672. При этом отметим, что одному пользователю может принадлежать одновременно несколько кошельков, что заметно затрудняет проведение поисковых мероприятий.

2. «Яндекс.Деньги» – это электронный кошелек платежной системы ООО «ПС Яндекс. Деньги».

3. «Деньги @Mail.Ru» – это идентификатор электронной платежной системы ООО «Деньги.Мэйл.Ру».

Для получения информации о владельце электронного кошелька оперативному сотруднику необходимо подготовить и направить запрос, аналогичный направляемому для получения информации о владельце электронного почтового ящика.

В полученных ответах должна содержаться следующая информация:

– с каких IP-адресов осуществлялось управление данными кошелька;

– куда перечислены денежные средства.

При решении задач ОРД нередко возникает необходимость установления средств вычислительной техники по MAC-адресу. У каждой сетевой карты компьютера, ноутбука, планшета, смартфона имеется уникальный MAC-адрес, который присваивается производителем. Использование MAC-адреса при решении задач ОРД позволяет сотрудникам оперативных подразделений ОВД устанавливать фактическое местоположение обозначенных технических устройств.

Для установления MAC-адреса необходимо изучить документы от устройства либо направить в рамках ОРМ «Наведение справок» запрос интернет-провайдеру о месте подключения устройства.

При проведении ОРМ по установлению абонента устройства следует учитывать, что MAC-адрес сетевого устройства передается оператору связи только при непосредственном подключении устройства к оборудованию интернет-провайдера. Это означает, что в случаях подключения устройства к сети Интернет посредством использования промежуточного оборудования, к которому относится WiFi-роутер, ADSL-модем или USB-модем, MAC-адрес устройства оператору связи не передается. При этом следует учитывать, что пользователь самостоятельно может изменить значение MAC-адреса устройства, т. к. это не требует определенных навыков, умений либо специальных познаний.

Выводы и заключение

Подводя итог нашему исследованию, отметим, что одним из приоритетных направлений в деле совершенствования информационно-аналитического обеспечения ОРД должно выступать активное внедрение и повсеместное использование современных методов и средств добывания информации.

Сотрудники оперативных подразделений ОВД должны постоянно повышать уровень профессиональной квалификации в сфере современных методов получения цифровой информации и

активно использовать ресурсы сети Интернет в качестве приоритетного источника оперативно значимой информации. Одновременно они должны уметь использовать проверенные методы получения информации при выполнении оперативно-служебных задач по раскрытию преступлений, совершаемых с использованием цифровых технологий.

СПИСОК ИСТОЧНИКОВ

1. *Тимофеев, С. В., Арутюнян, В. Р.* О некоторых аспектах привлечения специалиста в ходе изъятия электронных носителей информации при проведении оперативно-розыскных мероприятий // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 108–114.

2. *Тимофеев, С. В., Лузько, Д. Н.* Особенности сбора оперативно-розыскной информации: международная и отечественная практика // Криминалистика: вчера, сегодня, завтра. 2022. № 3 (23). С. 132–141.

3. Цифровая валюта и цифровые финансовые права как предмет и средство совершения преступлений / О. П. Грибунов, П. В. Никонов, С. В. Пархоменко и др. Иркутск : Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2023. 170 с.

4. *Федотов, Н. Н.* Форензика – компьютерная криминалистика. М. : Юридический мир, 2007. 142 с.

5. *Левашова, О. В., Витюк, А. А.* Положения Конвенции Совета Европы о кибербезопасности // Закон и право. 2021. № 11. С. 128–130.

6. *Третьякова, Е. И., Трубкина, О. В.* Правовые проблемы расследования мошенничества с использованием электронных средств платежа // Криминалистика: вчера, сегодня, завтра. 2020. № 2 (14). С. 195–200.

7. *Тимофеев, С. В.* Деанонимизация пользователя сети Интернет как метод оперативно-розыскного противодействия наркопреступности // Юристъ-Правоведъ. 2020. № 2 (93). С. 170–174.

REFERENCES

1. *Timofeev, S. V., Arutyunyan V. R.* O nekotoryh aspektah privlecheniya specialista v hode iz"yatiya elektronnyh nositelej informacii pri provedenii operativno-rozysknyh meropriyatij [On some aspects of attracting a specialist during the seizure of electronic media during operational investigative activities]. Kriminalistika: vchera, segodnya, zavtra. – Forensic Science: Yesterday, Today, Tomorrow. 2020. no 1(13). Pp. 108-114. (in Russian).

2. *Timofeev, S. V., Luz'ko, D. N.* Osobennosti sbora operativno-rozysknoj informacii: mezhdunarodnaya i otechestvennaya praktika [Peculiarities of collecting operational-search information: international and domestic practice]. Kriminalistika: vchera, segodnya, zavtra. – Forensic science: yesterday, today, tomorrow. 2022. no 3(23). Pp. 132-141. (in Russian).

3. Cifrovaya valyuta i cifrovye finansovye prava kak predmet i sredstvo sovershenija prestuplenij [Digital currency and digital financial rights as a subject and means of committing crimes]. O. P. Gribunov, P. B. Nikonov, C. B. Parhomenko [i dr.]. – Irkutsk : Irkutskij yuridicheskij institut (filial) federal'nogo gosudarstvennogo kazennogo obrazovatel'nogo uchrezhdeniya vysshego obrazovaniya "Universitet prokuratury Rossijskoj Federacii", 2023. – 170 p. (in Russian).

4. *Fedotov, N. N.* Forenzika - komp'yuternaya kriminalistika [Forensics - computer forensics]. M.: YUridicheskij mir, 2007. 142 p. (in Russian).

5. *Levashova, O. V., Vityuk, A. A.* Polozheniya Konvencii Soveta Evropy o kiberbezopasnosti [Provisions of the Council of Europe Convention on Cybersecurity]. Zakon i pravo. – Law and Law. 2021. no. 11. Pp. 128-130. (in Russian).

6. *Tret'yakova, E. I., Trubkina, O. V.* Pravovye problemy rassledovaniya moshennichestva s ispol'zovaniem elektronnyh sredstv platezha [Legal problems of investigating fraud using electronic means of payment]. Kriminalistika: vchera, segodnya, zavtra. – Forensic science: yesterday, today, tomorrow. 2020. no 2(14). Pp. 195-200. (in Russian).

7. *Timofeev, S. V.* Deanonimizaciya pol'zovatelya seti internet kak metod operativno-rozysknogo protivodejstviya narkoprestupnosti [Deanonymization of an Internet user as a method of operational investigative counteraction to drug crime] YUrist-Pravoved. – Yurist-Pravoved. 2020. no 2(93). – Pp. 170-174. (in Russian).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Арипшев Ахмед Мухамедович, кандидат экономических наук, заместитель начальника кафедры огневой подготовки. Северо-Кавказский институт повышения квалификации (филиал) Краснодарского университета МВД России. 360016, Российская Федерация, г. Нальчик, ул. Мальбахова, 123.

Шондиров Руслан Хазраилович, преподаватель кафедры огневой подготовки. Северо-Кавказский университет (филиал) Краснодарского института МВД России. 360016, Российская Федерация, г. Нальчик, ул. Мальбахова, 123.

INFORMATION ABOUT THE AUTHORS

Akhmed M. Aripshev, candidate of economic sciences, deputy head of the fire training department. North Caucasus Institute for Advanced Studies (branch) of the Krasnodar University of the MIA of Russia. 123, st. Malbakhova, Nalchik, Russian Federation, 360016.

Ruslan Kh. Shondirov, teacher of the department of fire training. North Caucasus University (branch) of the Krasnodar Institute of the MIA of Russia, 123, st. Malbakhova, Nalchik, Russian Federation, 360016.