



УДК 343.985.7
МРНТИ 10.85.51

Т.М. Коржумбаева, С.М. Абижанов

*Алматинская академия Министерства внутренних дел Республики Казахстан
имени М. Есбұлатова, г. Алматы, Республика Казахстан*

ОСОБЕННОСТИ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ РАБОТЫ В ВЫЯВЛЕНИИ, ПРЕДУПРЕЖДЕНИИ И ПРЕСЕЧЕНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Аннотация. Современное и эффективное реагирование на вызовы преступного мира требует от правоохранительных органов применения новых, действенных методов в работе. Одним из направлений в этой деятельности может выступать сегодня – информационно-аналитическая работа, носящая поисково-разведывательный характер. В статье говорится о необходимости совершенствования законодательства, в сфере оперативно-розыскной деятельности, в связи, с чем предлагается расширить перечень общих оперативно-розыскных мероприятий, направленных на мониторинг телекоммуникационных сетей и систем. В связи с высоким криминогенным потенциалом преступлений в сфере информационных технологий, подобные системы мониторинга скрытых сегментов Интернета могут стать весьма перспективными. В то же время, поиск и сбор информации об интересующих лицах и фактах сопряжен со значительными сложностями, обусловленными отсутствием четких методик осуществления оперативно-розыскных мероприятий, что требует организационных и правовых основ развития данной деятельности.

Ключевые слова: информация; аналитическая работа; противодействие; технологии; технические средства; мониторинг сетей; интернет; Darknet.

Т.М. Коржумбаева, С.М. Әбіжанов

*Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы
Алматы академиясы, Алматы қ., Қазақстан Республикасы*

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР САЛАСЫНДАҒЫ ҚЫЛМЫСТАРДЫ АНЫҚТАУ, АЛДЫН АЛУ ЖӘНЕ ЖОЛЫН КЕСУДЕГІ АҚПАРАТТЫҚ-ТАЛДАМАЛЫҚ ЖҰМЫСТЫҢ ЕРЕКШЕЛІКТЕРІ

Аннотация. Қылмыстық әлемнің сын-тегеуріндеріне заманауи және тиімді ден қою құқық қорғау органдарынан жұмыста жаңа, пәрменді әдістерді қолдануды талап етеді. Бүгінгі таңда бұл қызметтегі бағыттардың бірі – іздеу-барлау сипатындағы ақпараттық-аналитикалық жұмыс болуы мүмкін. Мақалада жедел-ізвестіру қызметі саласындағы заңнаманы жетілдіру қажеттілігі туралы айтылады, осыған байланысты телекоммуникациялық желілер мен жүйелердің мониторингіне бағытталған жалпы жедел-ізвестіру іс-шараларының тізбесін кеңейту ұсынылады. Ақпараттық технологиялар саласындағы қылмыстардың жоғары криминогендік әлеуетіне байланысты Интернеттің жасырын сегменттерін бақылаудың мұндай жүйелері өте перспективалы болуы мүмкін. Сонымен бірге қызығушылық танытқан адамдар мен фактілер туралы ақпаратты іздеу және жинау жедел-ізвестіру іс-шараларын жүзеге асырудың нақты әдістемелерінің болмауына байланысты айтарлықтай қиындықтармен байланысты, бұл осы қызметті дамытудың ұйымдастырушылық және құқықтық негіздерін талап етеді.

Түйінді сөздер: ақпарат; аналитикалық жұмыс; қарсы әрекет; технологиялар; техникалық құралдар; желілерді бақылау; интернет; Darknet.



T.M. Korzhumbayeva, S.M. Abizhanov
*Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan
named after M. Esbulatov, Almaty c., the Republic of Kazakhstan*

FEATURES OF INFORMATION AND ANALYTICAL WORK IN DETECTION, PREVENTION AND SUPPRESSION CRIMES IN THE FIELD OF INFORMATION TECHNOLOGY

Abstract. Modern and effective response to the challenges of the criminal world requires law enforcement agencies to apply new, effective methods in their work. One of the directions in this activity can be today – information and analytical work, which is of a search and intelligence nature. The authors of the article state the need to improve legislation in the field of operational investigative activities, in connection with which it is proposed to expand the list of general operational investigative measures aimed at monitoring telecommunications networks and systems. Due to the high criminogenic potential of crimes in the field of information technology, such systems for monitoring hidden segments of the Internet can become very promising. At the same time, the search and collection of information about persons of interest and facts is fraught with significant difficulties due to the lack of clear methods for carrying out operational search activities, which requires organizational and legal foundations for the development of this activity.

Keywords: information; analytical work; counteraction; technologies; technical means; network monitoring; Internet; Darknet.

DOI: 10.52425/25187252_2023_29_93

Введение. Развитие глобальной сети Интернет привело к тому, что можно очень много различной информации получить простым поисковым запросом об интересующем человеке, которая размещена в свободном доступе и не защищена, которая может быть использована преступными элементами в преступных целях. Информации настолько бывает иногда много и разноречиво ее содержание, что препятствует получению объективной правдивой информации о лице.

В таких условиях В.С. Овчинский приходит к выводу о том, что развитие информационно-коммуникационных технологий и киберсреды предусматривает пересмотр основы организационно-правового функционирования правоохранительных структур, где особую роль играет использование новых технологий противодействия преступности, методов цифровых расследований, переподготовки сотрудников ведомственных органов [1, 124 стр.].

Сегодня много исследований проводятся по данной проблематике и проблемам использования возможностей информационно-телекоммуникационных

технологий в раскрытии преступлений посвящено много научных работ [2]; [3]; [4].

На этом фоне, в противодействии преступлениям в сфере высоких технологий принципиальное значение имеет налаженная информационно-аналитическая работа, а именно такое ее направление как разведывательно-поисковое.

Материалы и методология. В качестве методологической основы автором использованы общенаучные и частные методы познания. В работе применялся системный подход к анализу норм отечественного законодательства, методы сравнительно-правового, социологического, статистического исследования и другие. Основу исследования составили нормы действующего законодательства Республики Казахстан (далее – РК), в том числе Законы РК «Об информатизации», «О связи» и другие, международное законодательство, а также научные труды отечественных и зарубежных ученых. Широко представлено в статье международное право в сфере противодействия преступлениям в сфере информационных технологий.

Результаты и их обсуждение. Сегодня для активизации рассматриваемых



процессов в Казахстане необходимо создать соответствующую правовую базу, тем более, что международное и отечественное законодательство уже содержат первоначальную основу. Например, в 2000 году в городе Нью-Йорке принята Конвенция ООН против транснациональной организованной преступности, в которой отмечена важность применения компетентными органами специальных методов расследования в целях эффективного противодействия организованной преступности. В числе таких методов названы электронное наблюдение и иные формы наблюдения¹.

В начале 2000-х годов в соседней России делались попытки ввести в оперативно-розыскное законодательство новое оперативно-розыскное мероприятие (далее – ОРМ) – электронное наблюдение. Так, Ю.Н. Соколов предлагает понимать под ним «комплексное оперативно-техническое мероприятие, проводимое на основании судебного решения, заключающееся в конспиративном получении оперативно-техническими подразделениями субъектов оперативно-розыскной деятельности фактической или оперативно-значимой информации с помощью специальных технических средств, фиксирующих и копирующих названную информацию во время ее передачи объектами оперативной заинтересованности через единые сети электросвязи Российской Федерации» [5, 14 стр.].

В этом смысле представляет повышенный интерес еще одно ОРМ, присутствующее в Модельном законе «Об оперативно-розыскной деятельности» государств-участников СНГ – мониторинг информационно-телекоммуникационных сетей и систем. Под ним понимается

получение сведений, необходимых для решения конкретных задач оперативно-розыскной деятельности (далее – ОРД), и их фиксация путем наблюдения с применением специальных технических средств за характеристиками электромагнитных и других физических полей, возникающих при обработке информации в информационных системах и базах данных и ее передаче по сетям электрической связи, компьютерным сетям и иным телекоммуникационным системам².

Подобного рода ОРМ в Законе РК «Об оперативно-розыскной деятельности» нет, но о данном мониторинге говорится в Концепции кибербезопасности «Киберщит Казахстана» в качестве одного из принципов, что отражает актуальность подобных угроз для жизнедеятельности нашего государства. В ней отмечено, что для полноценной оценки состояния защищенности объектов информатизации с учетом характера деятельности киберпреступников и иностранных технических компьютерных разведок, рассчитывающих на самоуспокоенность и небрежность со стороны владельцев информационных ресурсов и систем, необходимо стремиться к непрерывному мониторингу состояния информационных систем и ресурсов техническими средствами контроля защищенности и проведению работы по выявлению каналов утечки информации³.

В то же время, действующее законодательство Казахстана даже частным структурам предоставляет право такого мониторинга. Так, Закон РК «Об информатизации» под мониторингом событий информационной безопасности понимает – постоянное наблюдение за объектом информатизации с целью выявления и идентификации событий

¹ Конвенция Организации Объединенных Наций против транснациональной организованной преступности: принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года [Электронный ресурс] – Режим доступа: https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml (дата обращения: 25.03.2023).

² Модельный закон «Об оперативно-розыскной деятельности» (новая редакция): принят на двадцать седьмом пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ (постановление №27-6 от 16 ноября 2006 года) [Электронный ресурс] – Режим доступа: <http://www.cisatc.org/1289/135/154/245> (дата обращения: 25.03.2023).

³ Концепция кибербезопасности («Киберщит Казахстана»): утверждена постановлением Правительства Республики Казахстан от 30 июня 2017 г. №407 [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/P1700000407> (дата обращения: 25.03.2023).



информационной безопасности⁴.

Это говорит о том, что сегодня необходимо законодательство РК привести в соответствие, чтобы была возможность своевременного и эффективного реагирования на подобного рода угрозы. В связи с этим необходимо внести изменения в Закон РК «Об оперативно-розыскной деятельности» и расширить перечень общих оперативно-розыскных мероприятий, таким как «мониторинг информационного пространства и информационной инфраструктуры».

Кроме того Закон РК «Об информатизации», расшифровывает понятие – общедоступные электронные информационные ресурсы, под которыми понимаются ресурсы, которые предоставляются или распространяются их собственником или владельцем без указания условий доступа или их использования, а также сведения, доступ к которым является свободным и не зависит от формы их представления и способа распространения⁵.

Таким образом, предлагаемое ОРМ может носить характер общего, то есть проводимого без санкции прокурора, по решению руководителя оперативного аппарата. Следует отметить, что из указанных электронных ресурсов может быть получена любая информация, в том числе касающаяся персональных данных. Согласно статьи 3 Закона РК «О персональных данных и их защите»: его действие не распространяется на отношения, возникающие при сборе, обработке и защите персональных данных в ходе ОРД⁶.

Такой подход вполне обоснован и связан непосредственно с особенностями работы оперативных сотрудников с цифровой информацией или цифровыми устройствами которым известны, так называемые специ-

альные категории вот этих персональных данных, в связи с чем отсутствует необходимость в санкционировании. Например, конкретизация IP-адреса, лица представляющего оперативный интерес – что также может проводиться без санкции.

В зарубежной судебной практике превалирует мнение о том, что все IP-адреса, в том числе и в анонимных сетях – это полностью публичная информация. В США в деле против Джея Михода, которого обвинили в распространении детской порнографии через сайт PlayPen, расположенного в Darknet, ФБР имело прямой доступ к управлению этим сайтом на протяжении 13 дней. Тогда силовики загрузили туда специальные скрипты, которые в сумме собрали информацию об IP-адресах около 1 300 посетителей ресурса. Вынося вердикт по тому делу, судья Роберт Брайан сравнил IP-адреса в Darknet с любым телефонным номером, который рано или поздно можно найти⁷.

В пользу именно такого подхода говорит и анализ казахстанского законодательства. Так, согласно Закона РК от 24 ноября 2015 года «Об информатизации», к электронным информационным ресурсам ограниченного доступа относятся те, которые содержат сведения, доступ к которым ограничен законами РК либо их собственником или владельцем в случаях, установленных законодательством⁸.

Что касается Darknet и других анонимных сетей, то они никак не регулируются отечественным законодательством. Отсюда следует очень важный вывод, что в данной сфере не требуется никаких специальных разрешений для проведения такого общего ОРМ, как мониторинг информационного пространства и информационной инфраструктуры.

⁴ Об информатизации: закон Республики Казахстан от 24 нояб. 2015 г. №418-V ЗРК [Электронный ресурс] – Режим доступа: <http://adilet.zan.kz/rus/docs/Z1500000418> (дата обращения: 25.03.2023).

⁵ Там же.

⁶ О персональных данных и их защите: закон Республики Казахстан от 21 мая 2013 г. №94-V [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=31396226#pos=78;-45 (дата обращения: 26.03.2023).

⁷ Как ученые деанонимизировали пользователей TOR по заказу Минобороны США [Электронный ресурс] – Режим доступа: <http://www.furur.me/furur/freedom/freedom/216803-tor-attack> (дата обращения: 26.03.2023).

⁸ Об информатизации: закон Республики Казахстан от 24 нояб. 2015 г. №418-V ЗРК [Электронный ресурс] – Режим доступа: <http://adilet.zan.kz/rus/docs/Z1500000418> (дата обращения: 25.03.2023).



В этой связи, российские эксперты, верно подмечают преимущество подобных инструментов, которое заключается в том, что оперативно-поисковая (разведывательная) деятельность в сфере и инфраструктуре может проводиться с наименьшим количеством ОРМ, затрагивающих права и свободы граждан.

Указанная деятельность может осуществляться по следующим направлениям:

1. Поиск по информационным ресурсам глобальных сетей с использованием поисковых систем Google, Yandex, Rambler и т.д. Проведение поисковых мероприятий позволяет выявлять сайты, связанные с преступными формированиями, а также сайты, на которых размещена запрещенная информация для общего сведения.

2. Поиск информации в отношении отдельных лиц, представляющих оперативный интерес, размещаемый ими на своих страницах в социальных сетях.

3. Применение контент-анализа. Его особенность состоит в том, что он изучает документы в их социальном контексте. Этот метод может быть как главный, либо может использоваться с другими методами одновременно.

При этом, для мониторинга информационной активности фигурантов могут использоваться технологии автоматизированного сбора и анализа информации по принципу «больших данных» (big data) и интеллектуального анализа данных (data mining). Значительную помощь в этом оказывают специальные информационно-поисковые системы. Например, российские специалисты упоминают программное обеспечение Palantir, активно используемые ЦРУ и ФБР. Принцип работы, которого заключается в постоянной параллельной обработке всех доступных баз данных и анализе возможных связей по представленной там разной информации. После этого программа обобщает и отображает, с применением современных технологий визуализации данных, результаты анализа в удобном

формате, а также по заданным параметрам подозрительное поведение.

Вот конкретный пример из практики применения Palantir. В октябре 2011 года иностранный гражданин по имени Майк Фикри приобрел билет в один конец на самолет из Каира в Майами, где он снимал квартиру. В течении нескольких недель до того он неоднократно снимал ощутимые суммы со счета в российском банке и звонил нескольким абонентам в Сирию. Затем он арендовал грузовик, поехал в Орlando и в одиночку посетил Диснейленд. Там, как показали видеозаписи камер наблюдения, он не резвился среди аттракционов и достопримечательностей, а провел весь день, фотографируя на переполненной площадке при входе в парк. Ни одно из этих действий само по себе не вызывает подозрений. Только будучи взятые в комплексе, они наводят на подозрение. Все это было невозможно еще несколько лет назад, а сейчас работает на задачи безопасности [6].

Еще один аналогичный пример, но уже из России, показывает алгоритм проведения такого ОРМ, как «отождествление личности», то есть идентификация лица по индивидуализирующим статическим и динамическим неизменяемым признакам. В глобальной сети оно может осуществляться с использованием фотографий, отдельных анкетных данных, «ников», особенностей текстовых сообщений, аккаунтов конкретного лица и других информационных объектов. Так, на сайте по адресу pikabu.ru была создана группа под названием «Лига детективов». Один из посетителей сайта сфотографировал вид из своего окна и предложил определить его местонахождение. Фото осветили с помощью программы Photoshop. На заднем плане фотографии выявлено изображение церкви. В ходе поисковых мероприятий в сети Интернет были установлены отдельные аккаунты лица, разместившего фото: в онлайн-игре Dota, анкета в социальной сети «ВКонтакте» под вымышленными установочными данными. Таким образом,



был установлен город проживания – Тула. В ходе анализа особенностей изображения церкви и других церквей в городе Тула было установлено, что на фотографии изображена церковь Софии Премудрости Божией в Тульской семинарии. С использованием спутниковой карты установлено, что фото сделано из окна конкретного многоэтажного дома, что впоследствии было подтверждено автором фотографии [7, 194 стр.].

Вот пример из отечественной правоприменительной практики. Преступники использовали мошенническую схему по продаже запчастей на элитные автомашины с использованием сайта «Колеса.kz». Все телефонные номера с сайта были проанализированы посредством мессенджера «WhatsApp», и по одному из номеров получено фото молодой пары. В ходе ОРМ была установлена их личность. Затем через акционерное общество «Казахтелеком» были выявлены IP-адреса, с которых осуществлялось размещение объявлений, которые исходили с конкретного адреса квартиры в городе Костанай, которая сдавалась в аренду. Через ее владельца были установлены арендаторы, которые оказались преступниками. В то же время, следует отметить, что специализированные поисковые информационные системы отечественными правоохранителями не применялись.

При этом, как отмечают российские специалисты, хотя у них и приобретаются зарубежные разработки, наряду с ними используется собственные программные продукты.

Принцип действия информационно-поисковых программ основан на том, что при использовании Интернета пользователи оставляют следы своей деятельности, например, регистрация на различных ресурсах с одинаковым либо похожим «ником», использование каких-либо устойчивых фраз и выражений и др. На основании информации, полученной в результате такого мониторинга, осуществляются дальнейшие мероприятия по идентификации интересующих

фигурантов. Это может быть:

- обращение к Интернет-провайдерам и операторам связи, использование сервиса WHOIS (who is) – автоматизированной системы, предоставляющей публичный доступ к информации о доменном имени и его администраторе;
- изучение статистики посещения сайтов, имеющих отношение к противоправной деятельности, с целью выявления посещающих их лиц;
- изучение статистики работы пользователя для выявления посещаемых интернет-ресурсов;
- установление через оператора связи IP-адреса выявленного пользователя [7, С. 186-187].

Кроме того, для оперативных аппаратов представляют особый интерес такая опция, как создание так называемой «виртуальной личности» и проведение с ее помощью ОРМ (внедрение и имитация преступной деятельности). Технический прогресс позволил приблизиться к цели по достижению всестороннего, полного и объективного исследования обстоятельств по делу [8, 84 стр.].

Вместе с тем, анализ практики, показывает, что в повседневной деятельности оперативные сотрудники, перечисленные методы практически не используют, что вполне объяснимо – подобные методики еще не разработаны. Более того, традиционные методики ОРД пока также не адаптированы к специфике преступлений в сфере информационных технологий, а аналитическая работа организована очень слабо или вообще отсутствует.

Между тем, как правило, присутствие человека во всевозможных социальных сетях и Интернет-сервисах можно легко обнаружить, зная его «ник», то есть его некий уникальный идентификатор [9].

Часто люди его формируют при создании личной электронной почты, а затем используют в различных Интернет-сервисах. Автоматически проверить наличие пользователя в различных ресурсах можно, например, с помощью



такого сервиса, как <https://namechk.com/>, а современные поисковые машины обладают развитым языком запросов, позволяющим сузить критерии поиска информации. Далее с помощью специальных программ из полученных первичных данных можно извлечь углубленную информацию для ее анализа [10, 71 стр.].

Полученные в результате анализа сведения о разыскиваемом субъекте должны быть тщательно проанализированы, изучены, оценены. Чем больше будет отобрано данных, характеризующих преступника, тем легче перейти к версии о его виновности. При анализе и оценке выявленных признаков лица следует иметь в виду, что чем специфичнее тот или иной признак, чем реже он встречается, тем больше его поисковое значение, тем важнее содержащаяся в нем информация способная установить его индивидуальные особенности.

На протяжении всего процесса раскрытия, лицо, осуществляющее аналитический поиск должен стремиться пополнить совокупность признаков, характеризующих лицо, представляющее оперативный интерес. При этом признаки, уже установленные следствием, могут дополняться признаками, логически вытекающими из доказанных по делу фактов. Только после тщательного анализа выявленных признаков могут быть разработаны мероприятия, направленные на розыск и задержание преступника.

В целом эффективность информационно-аналитической работы для розыскной деятельности определяется:

- эффективностью этапа сбора информации представляющей оперативный интерес;
- полнотой и качеством информации;
- эффективностью использования полученных данных при проведении оперативно-розыскной деятельности.

Проанализированные возможности полученной информации, которая может являться источниками как доказательственной, так и ориентирующей информации при раскрытии данных

преступлений, позволяет расширить информационную базу, направленную на розыск преступника. В этой связи может быть систематизирована данная информация, и использована в розыскных целях. Вышеизложенное свидетельствует о том, что информация, собранная данным методом, должна быть систематизирована применительно к лицам, эпизодам преступной деятельности, проанализирована с тем, чтобы на последующем этапе ее можно было конкретизировать в целях выявления всех эпизодов преступной деятельности, установления соучастников, нанесенного материального ущерба, каналов его реализации, причин и условий, способствовавших совершению.

Во всех случаях полученные сведения должны способствовать эффективности проведения последующих следственных действий и ОРМ, розыска лица, подлежащего привлечению в качестве обвиняемого (если он не был установлен), похищенного имущества и др.

Заключение. В связи с высоким криминогенным потенциалом преступлений в сфере высоких технологий, подобные системы мониторинга скрытых сегментов Интернета могут стать весьма перспективными. В то же время, поиск и сбор информации об интересующих лицах и фактах сопряжен со значительными сложностями, обусловленными отсутствием четких методик осуществления ОРМ. Это подтверждают исследования, которые свидетельствуют о том, что оперативные сотрудники подразделений по борьбе с киберпреступлениями ОВД не представляют алгоритма такого мониторинга.

Между тем, вопросы своевременного выявления высокотехнологичных преступлений становятся с каждым днем все более актуальными, особенно в сфере повсеместного распространения широкополосного интернет-доступа. Можно применить самые совершенные средства аутентификации и криптования, отгородиться мощными системами безопасности, но одна маленькая оплошность в



ответственной программе способна свести на нет все усилия, предоставив квалифицированному злоумышленнику возможность задействовать эту оплошность в своих целях и в конце концов получить несанкционированные права доступа [11, 415 стр.].

Таким образом, подводя итоги рассмотрению особенностей информационно-аналитического обеспечения раскрытия и расследования преступлений в сфере информационных технологий и аспектов деятельности правоохранительных органов по их выявлению, можно прийти к следующим выводам:

1. Экспоненциальное увеличение числа пользователей казахстанского сегмента Интернета в последние годы ставит актуальную проблему изменения подхода отечественной правоохранительной

деятельности в сторону разработки принципиально новых методик выявления высокотехнологичных преступлений, прежде всего путем совершенствования оперативно-розыскного законодательства.

2. Такие методики уже созданы и успешно себя показали в развитых странах, которые в значительной степени научились контролировать криминальные проявления в глобальной сети. Изучение этого опыта наглядно показывает, что наиболее важное значение при этом имеет превентивная разведывательно-поисковая работа, прежде всего в анонимных информационных сетях.

3. Имеющийся зарубежный опыт позволяет создать организационные и правовые основы не только выявления, но и предупреждения, а также пресечения преступлений в сфере информационных технологий.

Список использованной литературы:

1. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. – М.: Норма, 2017. – 528 с.
2. Озеров, К.И. Раскрытие мошенничеств с использованием информационно-телекоммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. – 2021. – №1(89). – С. 167-171.
3. Евдокимов, К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: автореф. дис. ... д-ра. юрид. наук / К.Н. Евдокимов. – Москва, 2022. – 73 с.
4. Алексеенко, С.П. Использование баз данных при раскрытии преступлений в сфере информационно-телекоммуникационных технологий / С.П. Алексеенко, В.В. Достов, О.В. Пименова // Вестник Воронежского университета МВД России. – 2021. – №4. – С. 68-75.
5. Соколов, Ю.Н. Использование результатов электронного наблюдения в уголовном судопроизводстве и оперативно-розыскной деятельности: дис. ... канд. юрид. наук / Ю.Н. Соколов. – Екатеринбург, 2004 – 209 с.
6. A. Vance and B. Stone. Palantir, the War on Terror's Secret Weapon [Electronic resource] // Bloomberg Businessweek. – November 22, 2011. – Access mode: <https://www.bloomberg.com/news/articles/2011-11-22/palantir-the-war-on-terrors-secret-weapon> (Access data: 25.03.2023).
7. Сундиев, И.Ю. Теория и практика информационного противодействия экстремистской и террористической деятельности: монография / И.Ю. Сундиев, и др. – М.: ВНИИ МВД РФ, 2014. – 233 с.
8. Оракбаев, А.Б. О некоторых вопросах расследования убийств с использованием системы виртуализации / А.Б. Оракбаев // Құқық қорғау органдары академиясының жаршысы. – 2023. – №1(27). – С. 81-90.
9. Bowman, M. Reasoning about naming systems / M. Bowman, S.K. Debray, L.L. Peterson // ACM Trans. Program. Lang. Syst. – 1993. – №5(15). – Pp. 795-825.
10. Handbook of Asian Criminology / eds Jianhong Liu, Bill Heberton, Susyan Jou. – New York: Springer Science: Springer Business Media, 2013. – 445 p.



11. Lakbayev, K.S. The crimes in the field of high technology: concept, problems and methods of counteraction in Kazakhstan [Electronic resource] / K.S. Lakbayev, et al. // Int. J. Electronic Security and Digital Forensics. – 2020. – №4(12). – Pp. 412-423. – Access mode: <https://www.inderscience.com/info/inarticle.php?artid=110651> (Access data: 27.03.2023).

References:

1. Osnovy bor'by s kiberprestupnost'ju i kiberterrorizmom: hrestomatija / sost. V.S. Ovchinskij. – M.: Norma, 2017. – 528 s.
2. Ozerov, K.I. Raskrytie moshennichestv s ispol'zovaniem informacionno-telekommunikacionnyh tehnologij // Vestnik Sankt-Peterburgskogo universiteta MVD Rossii. – 2021. – №1(89). – С. 167-171.
3. Evdokimov, K.N. Protivodejstvie komp'yuternoj prestupnosti: teorija, zakonodatel'stvo, praktika: avtoref. dis. ... d-ra. jurid. nauk / K.N. Evdokimov. – Moskva, 2022. – 73 s.
4. Alekseenko, S.P. Ispol'zovanie baz dannyh pri raskrytii prestuplenij v sfere informacionno-telekommunikacionnyh tehnologij / S.P. Alekseenko, V.V. Dostov, O.V. Pimenova // Vestnik Voronezhskogo universiteta MVD Rossii. – 2021. – №4. – С. 68-75.
5. Sokolov, Ju.N. Ispol'zovanie rezul'tatov jelektronnogo nabljudenija v ugolovnom sudoproizvodstve i operativno-rozysknoj dejatel'nosti: dis. ... kand. jurid. nauk / Ju.N. Sokolov. – Ekaterinburg, 2004 – 209 s.
6. A. Vance and B. Stone. Palantir, the War on Terror's Secret Weapon [Electronic resource] // Bloomberg Businessweek. – November 22, 2011. – Access mode: <https://www.bloomberg.com/news/articles/2011-11-22/palantir-the-war-on-terrors-secret-weapon> (Access data: 25.03.2023).
7. Sundiev, I.Ju. Teorija i praktika informacionnogo protivodejstviya jekstremistskoj i terroristicheskoj dejatel'nosti: monografija / I.Ju. Sundiev, i dr. – M.: VNII MVD RF, 2014. – 233 s.
8. Orakbaev, A.B. O nekotoryh voprosah rassledovanija ubijstv s ispol'zovaniem sistemy virtualizacii / A.B. Orakbaev // Құқық қорғау органдары академиясының жаршысы. – 2023. – №1(27). – С. 81-90.
9. Bowman, M. Reasoning about naming systems / M. Bowman, S.K. Debray, L.L. Peterson // ACM Trans. Program. Lang. Syst. – 1993. – №5(15). – Pp. 795-825.
10. Handbook of Asian Criminology / eds Jianhong Liu, Bill Heberton, Susyan Jou. – New York: Springer Science: Springer Business Media, 2013. – 445 p.
11. Lakbayev, K.S. The crimes in the field of high technology: concept, problems and methods of counteraction in Kazakhstan [Electronic resource] / K.S. Lakbayev, et al. // Int. J. Electronic Security and Digital Forensics. – 2020. – №4(12). – Pp. 412-423. – Access mode: <https://www.inderscience.com/info/inarticle.php?artid=110651> (Access data: 27.03.2023).

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Тамара Муслиновна Коржумбаева – Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясының әкімшілік-құқықтық пәндер кафедрасының бастығы, заң ғылымдарының кандидаты, қауымдастырылған профессор, e-mail: deadpool69@mail.ru.

Коржумбаева Тамара Муслиновна – начальник кафедры административно-правовых дисциплин Алматинской академии Министерства внутренних дел Республики Казахстан имени М. Есбулатова, кандидат юридических наук, ассоциированный профессор, e-mail: deadpool69@mail.ru.

Korzhumbayeva Tamara Muslinovna – Head of the Department of Administrative and Legal Disciplines of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Candidate of Law, Associate Professor, e-mail: deadpool69@mail.ru.



Сырым Маратұлы Әбіжанов – Қазақстан Республикасы Ішкі істер министрлігінің М. Есболатов атындағы Алматы академиясының қылмыстық құқық және криминология кафедрасының доценті, философия докторы (PhD), e-mail: abizhanov@mail.ru.

Абижанов Сырым Маратович – доцент кафедры уголовного права и криминологии Алматинской академии Министерства внутренних дел Республики Казахстан имени М. Есбулатова, доктор философии (PhD), e-mail: abizhanov@mail.ru.

Abizhanov Syrym Maratovich – Associate Professor of the Department of Criminal Law and Criminology of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Doctor of Philosophy (PhD), e-mail: abizhanov@mail.ru.