Научная статья
УДК 351.74:004:03
https://doi.org/10.36511/2588-0071-2024-3-61-70

Цифровая трансформация информационных ресурсов в деятельности органов внутренних дел Российской Федерации

Наумов Юрий Геннадьевич[1], Стенюшкина Эльвира Андреевна[2]

[1, 2]Академия управления МВД России, Москва, Россия
[1]naumov6112@rambler.ru
[2]1359364@list.ru

Аннотация

В статье представлен экономический анализ развития цифровой трансформации органов внутренних дел. Описаны достижения и перспективные направления в области внедрения в правоохранительную деятельность цифровых технологий, возникающие проблемы и пути решения на примере передового опыта зарубежных стран.

Ключевые слова: цифровая трансформация; цифровые технологии; технологии искусственного интеллекта, программно-аппаратные комплексы

Для цитирования

Наумов Ю. Г., Стенюшкина Э. А. Цифровая трансформация информационных ресурсов в деятельности органов внутренних дел Российской Федерации // На страже экономики. 2024. № 3 (30). С. 61–70. https://doi.org/10.36511/2588-0071-2024-3-61-70.

Original article

Digital transformation of information resources in the activities of the internal affairs bodies of the Russian Federation

Yuri G. Naumov[1], Elvira A. Stenyushkina[2]

[1, 2]Academy of Management of the Ministry of Internal Affairs of Russia, Moscow, Russian Federation
[1]naumov6112@rambler.ru
[2]1359364@list.ru

Abstract

The article presents an analysis of the development of the digital transformation of internal affairs bodies. The achievements and promising directions in the field of the introduction of digital technologies into law enforcement, emerging problems and solutions are described using the example of the best practices of foreign countries.

Keywords: digital transformation; digital technologies; artificial intelligence technologies

For citation
Naumov Yu. G., Stenyushkina E. A. Digital transformation of information resources in the activities of the internal affairs bodies of the Russian Federation. *The Economy under Guard,* 2024, no. 3 (30), pp. 61–70. (In Russ.). https://doi.org/10.36511/2588-0071-2024-3-61-70.

Анализ развития цифровой трансформации служб полиции показывает, что эффективность их деятельности напрямую зависит от сетевой формы вовлечения многочисленных ресурсов для решения правоохранительных задач.

С принятием программы «О стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» важным вопросом стало развитие программы «Цифровая экономика Российской Федерации» [1]. В связи с этим цифровые технологии более интенсивно внедряются практически во все сферы жизни общества, при этом правовая основа, защита от утечки информации, методика предотвращения и раскрытия преступлений находятся не на должном уровне.

Число компьютерных пользователей в 2023 году увеличилось во много раз и продолжает увеличиваться, в том числе в МВД России. При этом необходимо отметить тот факт, что интенсивное использование компьютерных технологий имеет как положительный, так и отрицательный эффект.

Согласно статистическим данным (сборник ФКУ «ГИАЦ МВД России “О состоянии преступности в Российской Федерации за январь–октябрь 2023 года”») в январе – декабре 2023 года оперативная обстановка на территории Российской Федерации в сфере информационно-телекоммуникационных технологий (далее — ИТТ) характеризовалась значительным увеличением (на 29,8 %) количества преступлений, зарегистрированных органами внутренних дел (с 515 021 до 668 719), в то же время количество тяжких и особо тяжких преступлений увеличилось на 26 % (с 268 450 до 338 270).

Несмотря на незначительное снижение общего количества зарегистрированных преступлений (–1 %; с 1 966 759 до 1 947 161), удельный вес ИТТ-преступлений увеличился на 8,1 % и составил 34,3 %.

На 66,2 % увеличился размер материального ущерба, причиненного противоправными деяниями, совершенными с использованием ИТТ (с 91,9 до 152,7 млрд рублей). По расследованным уголовным делам общая сумма возмещенного ущерба, включая наложение ареста на имущество, составила 43 млрд рублей (28,1 % от причиненного ущерба).

Активизировалась работа по выявлению групповых ИТТ-преступлений. Так, противоправных деяний рассматриваемой категории, совершенных группой лиц по предварительному сговору, выявлено 37 610 (+68,6; 2022 г. — 22 305), совершенных организованной группой либо преступным сообществом — 21 478 (+29,9 %; 2022 г. — 16 534).

На 9 % увеличилось количество выявленных лиц, совершивших ИТТ-преступления (с 93 769 до 102 169).

Значительную часть (72,7 %) от общего массива ИТТ-преступлений составляют противоправные деяния против собственности, число которых составило 486 087 (+27,9 %; 2022 г. — 380 034). Также наблюдается рост зарегистрированных преступлений в сфере незаконного оборота наркотиков на 25,9 %

(101 993, 2022 г. — 81 038) и экономической направленности на 7 % (21 532; 2022 г. — 20 113).

Значительно увеличилось количество криминальных деяний в сфере компьютерной информации (в 3,9 раза; с 9 431 до 36 431). Практически все преступления данной категории (36 274; 2022 г. — 8 884) связаны с неправомерным доступом к компьютерной информации, из них лица установлены по 1 200 преступлениям (ЭБиПК — 61, УУР — 117, СТМ — 415, ПБК — 518), при этом по 26 024 фактам приняты решения о приостановлении уголовных дел по пунктам 1–4 части 1 статьи 208 Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ).

Увеличение преступлений в сфере компьютерной информации (гл. 28 УК РФ) обусловлено применением требований Верховного Суда Российской Федерации [2] о дополнительной квалификации мошенничеств, совершенных посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, по статьям 272, 273 или 274.1 УК РФ.

Стоит отметить снижение на 17,3 % количества зарегистрированных заведомо ложных сообщений об акте терроризма (с 21 033 до 17 392). В отчетном периоде лица установлены по 758 фактам (УУР — 425, ППЭ — 149, ПБК — 35) и по 16 444 фактам приняты решения о приостановлении уголовных дел по пунктам 1–4 части 1 статьи 208 УПК РФ.

В текущем периоде при совершении ИТТ-преступлений в 2,2 раза активнее стали использоваться средства мгновенного обмена сообщениями (интернет-мессенджеры) (с 70 794 до 155 378).

Отмечается рост фактов использования в противоправной деятельности программных средств на 63,3 % (11 752; 2022 г. — 7 198), методов социальной инженерии на 48,8 % (106 830; 2022 г. — 71 805), средств мобильной связи на 42,3 % (301 144; 2022 г. — 211 606), сети «Интернет» на 39,2 % (503 275; 2022 г. —361 591), компьютерной техники на 26,6 % (34 617; 2022 г. — 27 354) и электронных платежных систем 23,4 % (29 547; 2022 г. — 23 944).

При этом сократилось на 38,4 % число выявленных преступных деяний, при совершении которых использовалась *SIP*-телефония (с 14 018 до 8 640).

За указанный период на 66,9 % увеличилось количество ИТТ-преступлений, совершенных в отношении пенсионеров (с 67 766 до 113 104) и на 27,7 % — несовершеннолетних (с 5 327 до 6 803).

В 2023 году подразделениями по борьбе с противоправным использованием информационных-телекоммуникационных технологий (далее — ИКТ) МВД России выявлено 4 776 преступлений, совершенных с использованием ИКТ, из которых в сфере половой неприкосновенности — 1 304 (ст. 132, 133, 134, 135, 242.1, 242.2 УК РФ), преступлений против собственности — 1 994 (ст. 158, 159, 163 УК РФ) и преступлений в сфере компьютерной информации — 945 (ст. 272, 273, 274 УК РФ).

Расследовано 1 974 преступления в сфере противоправного использования ИКТ. Лица установлены по 3 522 ИКТ-преступлениям, из которых против половой неприкосновенности — 1 020 (ст. 132, 133, 134, 135, 242.1, 242.2 УК РФ), преступлений против собственности — 1 484 (ст. 158, 159, 163 УК РФ) и в сфере компьютерной информации — 552 (ст. 272, 273, 274 УК РФ).

Привлечено к уголовной ответственности 648 лиц.

Большое влияние на увеличение количества преступлений, совершаемых с использованием IT-технологий, оказывает расширение области применения цифровых средств платежа при расчетах за приобретаемые товары и услуги, а также пренебрежение средствами защиты персональных данных субъектами их обработки.

В целях профилактики киберпреступности используются мониторинговые программно-аппаратные комплексы социальных сетей, такие как: «Сеус лаб», «Крибрум», «Глаз Бога», «Буратино», «Лев Толстой», «*IP*-поиск» и другие.

Так, «Крибрум» — программно-аппаратный комплекс, который позволяет собрать данные из социальных сетей и СМИ в реальном времени, 60 % информации собирается около часа. Собранная информация не удаляется, хранится с 2014 года. Анализ проводится на 23 языках. Программно-аппаратный комплекс анализирует следующие источники данных: *Facebook*, *Instagram*, ВКонтакте, Одноклассники, *TikTok*, *Twitter*, *YouTube*, *Telegram*-каналы (блоги, форумы, чаты, интернет-СМИ, сайты госорганов, ленты информагенств и другие тематические порталы). «Крибрум» позволяет проанализировать отдельных пользователей, аккаунты, связь между пользователями или аккаунтами, выявить противоправное поведение, в том числе автоматически составлять досье по конкретному автору, включая удаленную информацию, выявлять интересы и наклонности сообщества, анализировать связи пользователей с его возможным окружением, выявлять психологические портреты (девиантное поведение, склонность к терроризму, экстремизму, наркотикам, насилию, призывы к несогласованным публичным мероприятиям). Позволяет провести поиск по изображениям и лицам: идентификация личности по фото, определение первоисточников фотоизображения. Поиск по символам позволяет выявить следующую информацию: запрещенную символику дискредитирующих материалов, первоисточника фотографии. Программный комплекс позволяет проанализировать уровень социальной напряженности, в том числе выявлять основные причины роста социальной напряженности, уровень недовольства граждан по различным аспектам, а также активистов, которые эксплуатируют проблемы граждан.

Стоимость использования данного программного комплекса составляет 500 000 рублей в год, при этом исследоваться будет до 5 объектов, от 5–15 объектов составит 972 000 рублей в год, 15–30 составит 1 605 000 рублей в год, 30–50 — 2 568 000 рублей в год, неограниченное количество объектов по одной теме для одного заказчика составит 7 200 000 рублей в год, неограниченное количество объектов, групп объектов, тем для одного заказчика составит 25 200 000 рублей в год. Под объектом следует понимать все синонимы и виды написания.

Веб-приложение «СЕУС» позволяет пользователю вести мониторинг и анализ информации, размещенной в открытом доступе в социальных сетях «ВКонтакте», «Одноклассники», а также мессенджеров «Telegram», «Сигнал». По ключевым словам и словосочетаниям приложение позволяет выявить пользователей, размещавших противоправную информацию в своих профилях, отследить активность профиля, изменения профиля и определить их географическую принадлежность. По данным СМИ, данное приложение используется в 20 регионах в правоохранительной деятельности, однако проведенным опросом

установлено, что на районном уровне о подобных программных комплексах слышат впервые и мониторинг осуществляется вручную.

«Глаз Бога» — бот, позволяющий осуществлять поиск информации из открытых источников. Так, по фото человека в социальных сетях «ВКонтакте» или «Одноклассники» бот использует нейронную сеть, чтобы обнаруживать уникальные характеристики лица, чтобы затем находить похожие лица в базе. По номеру телефона бот ищет возможные имена, Ф. И. О, объявления и социальные сети, привязанные к данному номеру из открытых источников. По идентификационному номеру *VIN* или госномеру автомобиля предоставляет информацию о страховках, объявлениях о возможных продажах авто, технических характеристиках и всех владельцах транспортного средства.

Данный бот будет полезен, если в первые часы после угона автомобиля номер телефона появится в объявлениях о продаже угнанного автомобиля. Еще одна полезная функция — поиск аккаунтов по их местоположению, информация предоставляется о пользователях *Telegram*, которые в данный момент находятся рядом с выбранной пользователем точкой геопозиции. Пользование данной системой осуществляется по подписке (100 рублей в день и 2 500 рублей за 180 дней). В МВД России пользование данным ботом не предусмотрено, однако любой пользователь может зарегистрироваться на сайте, оплатить пользование и получить интересующую информацию.

Информационно-аналитическая система «Буратино» — поиск информации из открытых источников, в том числе социальных сетей. Основные задачи данной системы — профилактика корпоративной коррупции, злоупотреблений должностным положением и мошенничества, обеспечение кадровой безопасности, профилактика конфликта интересов и ряда других. При этом разработчик обучает будущих пользователей работе с данной системой. Стоимость обслуживания и обучения рассчитывается для каждой организации, ведомства индивидуально.

Одной из полезных, на наш взгляд, является программа «Георгий Победоносец», которая позволяет отслеживать информацию о вовлечении детей в экстремистские и террористические группировки, колумбайн, пропаганде суицида среди несовершеннолетних. Программа с помощью искусственного интеллекта позволяет отслеживать в автоматическом режиме вступление детей в опасные субкультуры. Создание системы оценили в 200 млн рублей, ежегодная поддержка составит 100 млн рублей, стоимость подключения одному региону может обойтись от 1 до 5 млн ежегодно.

IP-поиск позволяет массово проверять *IP*-адреса и их географические данные. Полезен для правоохранителей тем, что позволяет установить точное местоположение лиц.

В настоящее время иностранные социальные сети были заблокированы Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций, но пользователи из России продолжают пользоваться данными социальными сетями через *VPN*-сервис, при этом *ID* пользователя будет находиться в другой стране, а пользователь продолжает вести переписку о противоправных действиях в России. Поэтому вышеперечисленные программы мониторинга социальных сетей продолжают работать только в отношении российских социальных сетей.

В США и Израиле успешно применяется программа *Zencity*, которая позволяет отслеживать протестную активность населения — самостоятельно определяет потенциальные риски правонарушительства, анализирует публичные материалы и в установленном виде формирует отчеты.

Внедрение такого уровня программ по мониторингу социальных сетей в деятельность правоохранительных органов актуализирует профилактику преступлений и его причинного арсенала условий, способствующих их совершению (социально-экономические, социально-психологические, воспитательные, правовые и организационно-управленческие причины и иные) [3].

На примере территориального ОМВД по Энскому району г. Москвы более подробно рассмотрим организационно-экономические причины цифровой преступности. Так, на территории обслуживания ОМВД по Энскому району проживает 135 659 жителей. Ежедневно регистрируется более 120 правонарушений и преступлений, в том числе более 20 совершаются с помощью информационных технологий.

Уточним, что ни один сотрудник указанного ОМВД не имеет в наличии программ для мониторинга социальных сетей, что существенно затрудняет анализ оперативной обстановки. Вместе с тем в отдел было закуплено 37 мобильных планшетов «Самсунг» стоимостью 16 тысяч рублей. В данных планшетах установлена автоматизированная система ИСОД (обработки информации, программно-аппаратных комплексов, программно-технических средств, систем связи и передачи данных). При помощи данных планшетов патрульно-постовая служба полиции (12 планшетов) и участковые уполномоченные полиции (25 планшетов) осуществляют доступ к информационным ресурсам с помощью 3*G*/4*G* сети операторов связи.

Отмечая положительные стороны использования мобильных планшетов, необходимо сказать, что их применение в правоохранительной деятельности имеет ряд сложностей:

— ограниченное время действия зарядного устройства;

— перебои связи, а следовательно, отсутствие входа в подсистемы при перемещении с мобильными планшетами по территории обслуживания;

— отсутствие для сотрудников возможности самостоятельной проверки на наличие вредоносных программ;

— программное обеспечение в планшетах необходимо периодически обновлять, для этого необходим ключ для доступа в ИСОД, стоимость одного ключа составляет 2 500 рублей. На примере выбранного отдела необходимо 234 ключа (количество сотрудников, имеющих доступ к ИСОД, в том числе со стационарного рабочего места), что составит 585 000 и сам ключ-флэш — носитель стоит 1 000 рублей, а это еще 234 000 рублей. При установке несертифицированного программного обеспечения проводятся служебные проверки с привлечением пользователей мобильных устройств к дисциплинарной ответственности.

Еще одним существенным, на наш взгляд, недостатком мобильных планшетов, используемых в МВД России, является отсутствие возможности ознакомиться с протоколами об административных правонарушениях привлекаемым к административной ответственности лицам. В связи с этим при выявлении правонарушения сотрудники патрульно-постовой службы или участковый уполно-

моченный полиции обязаны доставить правонарушителя в участковый пункт полиции или в дежурную часть, составить рукописный протокол, предоставить правонарушителю его для ознакомления и далее передать в группу по исполнению административного законодательства для внесения данного протокола в модуль СООП «Административная практика».

В соответствии с приказом МВД России от 30 августа 2017 года «О должностных лицах системы Министерства внутренних дел Российской Федерации, уполномоченных составлять протоколы об административных правонарушениях и осуществлять административное задержание» [4] участковые уполномоченные полиции и сотрудники патрульно-постовой службы полиции наделены правом составления протоколов об административных правонарушениях. При этом необходимо отметить, что временной ресурс значимо сокращается при оформлении административных материалов.

Например, в Казахстане при закупке мобильных планшетов возможность ознакомления правонарушителя с протоколом об административном правонарушении первоначально учитывалась, поэтому в настоящее время планшеты закуплены вместе со стилусами, которые позволяют правонарушителям расписаться в мобильном планшете, что значительно экономит время [5].

На наш взгляд, данная проблема может быть разрешена либо закупкой новых планшетов со стилусами, либо изменениями в нормативных правовых актах о наличии электронной подписи у граждан и хранении ее не на флэш-носителе, а в облачном хранилище данных, доступ к которому технически будет осуществляться через мобильный планшет сотрудника полиции одновременно при ознакомлении с протоколом об административном правонарушении.

Положительным направлением в правоохранительной деятельности является подключение программного обеспечения, в том числе мобильных планшетов, к Единому центру хранения данных (далее – ЕЦХД), который управляется Департаментом информационных технологий. Это позволяет просмотреть изображение с любой камеры, подключенной к городской системе видеонаблюдения. ЕЦХД применяется для восстановления события правонарушения, преступления, для предоставления в качестве доказательства в суд, для распознавания лиц вручную, если уже составлен фоторобот или свидетель, потерпевший указал на подозреваемого. Сотрудник полиции с помощью ЕЦХД осуществляет сверку подозреваемого лица с изображением лица на месте преступления. В настоящее время Департамент информационных технологий объявил тендер о подключении к ЕЦХД регионов, но видео будет храниться в г. Москве, так как пока нет централизованного решения для хранения видеоаналитики. Данное направление в деятельности полиции при подключении всех субъектов поможет значительно повысить раскрываемость преступлений.

При расследовании преступлений, совершаемых с помощью информационных технологий, продолжает оставаться одним из проблемных вопросов длительный и сложный процесс получения необходимой информации на запросы от интернет-провайдеров, операторов связи, кредитных учреждений.

В настоящее время идет проработка вопроса ПАО «Сбербанк» о сокращении сроков и автоматизации исполнения запросов, направляемых в электронной форме. По результатам указанного взаимодействия со СберКорус (ООО «КОРУС

Консалтинг СНГ») достигнута договоренность об использовании баз данных банков и операторов связи правоохранительными органами. В частности, СберКорус разработана система предоставления сведений МВД России. В настоящее время в систему включены ПАО «Сбербанк» и ПАО «Альфа-Банк», планируется подключение Банка России, ПАО «Совкомбанк», АО «Россельхозбанк», АО «Т-Банк». В настоящее время срок исполнения запросов достигает от 10 до 30 дней.

На примере рассматриваемого территориального органа мы можем наблюдать только то, что ответы на запросы поступают длительное время. Так, в соответствии с приказом МВД России от 29 декабря 2020 года № 925 «Об утверждении Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество ПТК "ИБД-Ф"» [6] соответствующими подразделениями МВД России вносятся реквизиты сайтов и номера телефонов, с которых было осуществлено предполагаемое преступление, однако из-за длительного ответа на запросы пропадает оперативность локализации преступлений.

С учетом изложенного любая служебная информация и программное обеспечение нуждаются в оценке рисков внедряемых ресурсов.

Экономическое обоснование на внедрение и защиту информационных ресурсов должно иметь рациональный и прагматический подход, имеющийся в такой современной технологии, как форсайт, позволяющей планировать ресурсное обеспечение органов внутренних дел из будущего в настоящем. При этом главным отличием технологий форсайт от стратегического планирования является то, что стратегия исходит из оценки имеющихся ресурсов в настоящее время, а форсайт — их движения от будущего к настоящему [7].

Современный формат развития цифровых технологий в правоохранительной деятельности страны должен быть направлен в первую очередь на профилактику и снижение резонансной преступности. Поэтому проблемы вовлечения многочисленных сетевых ресурсов для решения правоохранительных задач должны решаться оперативно и качественно.

Другой задачей должно являться достижение соглашений по межведомственному взаимодействию в режиме реального времени интернет-провайдеров, операторов связи, кредитных учреждений и правоохранительных органов. Данная задача не требует больших затрат на логистику, но позволит значительно увеличить эффективность правоохранительного воздействия, в том числе по горячим следам.

Список источников

1. Паспорт национального проекта Национальная программа «Цифровая экономика Российской Федерации» (утверждена президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 года № 7). Доступ из СПС «КонсультантПлюс» (дата обращения: 23.06.2024).

2. О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48. Доступ из СПС «КонсультантПлюс» (дата обращения: 23.06.2024).

3. Ищук Я. Г., Пинкевич Т. В., Смольянинов Е. С. Цифровая Криминология: учебное пособие. Москва: Академия управления МВД России, 2021.

4. О должностных лицах системы Министерства внутренних дел Российской Федерации, уполномоченных составлять протоколы об административных правонарушениях и осуществлять административное задержание: приказ МВД России от 30 августа 2017 года № 685. Доступ из СПС «КонсультантПлюс» (дата обращения: 23.06.2024).

5. Об утверждении Правил ведения Единого реестра административных производств: приказ и. о. Генерального прокурора Республики Казахстан от 10 июля 2020 года № 85 (зарегистрирован в Министерстве юстиции Республики Казахстан 14 июля 2020 года № 20962). URL: https://adilet.zan.kz/rus/docs (дата обращения: 23.06.2024).

6. Об утверждении Временной инструкции по формированию, ведению и использованию подсистемы «Дистанционное мошенничество ПТК "ИБД-Ф"»: приказ МВД России от 29 декабря 2020 года № 925. Доступ из СПС «КонсультантПлюс» (дата обращения: 23.06.2024).

7. Тыловое и финансовое обеспечение органов внутренних дел Российской Федерации: учебник: в 2 ч. / К. Н. Алешин, Б. О. Баторов, С. Н. Белова [и др.]; под ред. К. Н. Алешина, Ю. Г. Наумова. Москва: Академия управления МВД России, 2023. Ч. 2.

References

1. National program "Digital Economy of the Russian Federation" approved by the minutes of the meeting of the Presidium of the Presidential Council for Strategic Development and National Projects no. 7 of dated June 4, 2019. Access from the reference legal system "ConsultantPlus" (accessed 23.06.2024). (In Russ.)

2. On judicial practice in cases of fraud, embezzlement and misappropriation: resolution of the Plenum of the Supreme Court of the Russian Federation no. 48 of dated November 30, 2017. Access from the reference legal system "ConsultantPlus" (accessed 23.06.2024). (In Russ.)

3. Ischuk Y. G., Pinkevich T. V., Smolyaninov E. S. Digital Criminology: textbook. Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, 2021. P. 47. (In Russ.)

4. On the issues of operation of modernized software for the implementation of the Service of public order protection: order of the Ministry of Internal Affairs of Russia no. 436 of dated June 21, 2022. Access from the reference legal system "ConsultantPlus" (accessed 23.06.2024). (In Russ.)

5. On approval of the Rules for maintaining the Unified Register of Administrative Proceedings Order of the Acting Prosecutor General of the Republic of Kazakhstan no. 85 of dated July 10, 2020. Registered with the Ministry of Justice of the Republic of Kazakhstan no 20962 of dated July 14, 2020. URL: https://adilet.zan.kz/rus/docs (accessed 23.06.2024). (In Russ.)

6. On Approval of the Temporary Instruction on the formation, maintenance and use of the subsystem "Remote fraud of the ITC «IBD – F»": order of the Ministry of Internal Affairs of Russia Order of the Ministry of Internal Affairs of Russia no. 925 of dated December 29, 2020. Access from the reference legal system "ConsultantPlus" (accessed 23.06.2024). (In Russ.)

7. Logistics and financial support of internal affairs bodies of the Russian Federation: textbook: in 2 parts / K. N. Alyoshin, B. O. Batorov, S. N. Belova [et al.]; ed. by K. N. Alyoshin, Y. G. Naumov. Moscow: Academy of Management of the Ministry of Internal Affairs of Russia, 2023. Ch. 2. (In Russ.)

Информация об авторах | Information about the authors

Ю. Г. Наумов — доктор экономических наук, профессор, профессор кафедры организации финансово-экономического, материально-технического и медицинского обеспечения Академии управления МВД России

Yu. G. Naumov — Doctor of Sciences (Economy), Professor, Professor of the Department of Organization of Financial and Economic, logistical and medical support Academy of Management of the Ministry of Internal Affairs of Russia

Э. А. Стенюшкина — адъюнкт 3 факультета Академии управления МВД России

E. A. Stenyushkina — Student of the 3nd faculty Academy of Management of the Ministry of Internal Affairs of Russia

Статья поступила в редакцию 10.06.2024; одобрена после рецензирования 17.08.2024; принята к публикации 24.09.2024.

The article was submitted 10.06.2024; approved after reviewing 17.08.2024; accepted for publication 24.09.2024.