

ХАРИСОВА Зарина Ирековна
Уфимский университет науки и технологий,
Уфа, Россия,
zarinaid@mail.ru,
<https://orcid.org/0000-0002-3902-3459>

KHARISOVA Zarina Irekovna
Ufa University of Science and Technology,
Ufa, Russia

ОСОБЕННОСТИ ОСМОТРА ИЗОЛИРОВАННОГО ПРОФИЛЯ («ВТОРОГО ПРОСТРАНСТВА») МОБИЛЬНОГО СРЕДСТВА СВЯЗИ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

FEATURES OF THE EXAMINATION OF THE ISOLATED PROFILE ("SECOND SPACE")
ON MOBILE DEVICES IN CYBERCRIME INVESTIGATIONS

Аннотация. При расследовании киберпреступлений и иных преступных деяний, совершаемых с использованием информационно-телекоммуникационных технологий, зачастую требуется производство осмотра мобильных средств связи, однако наличие в них функции формирования «второго пространства» (скрытого изолированного пользовательского профиля) может приводить к утрате имеющейся доказательственной базы. Прикладное значение исследования определяется возможностью выявления на практике механизмов изоляции данных, реализованных популярными сегодня производителями мобильных устройств (Samsung Secure Folder, MIUI (Xiaomi) Second Space, Magic UI Private Mode (Huawei и Honor)). Цель исследования: рассмотреть особенности обнаружения и осмотра скрытых рабочих пространств в мобильных средствах связи, активно используемых преступниками в противоправных целях. В процессе исследования использовалась совокупность общих (описания, обобщения и сравнения), общенаучных (анализа, синтеза) и частнонаучных (кибернетический, системного анализа, сравнительно-правовой) методов познания. Общие и общенаучные методы использовались при рассмотрении технической архитектуры изолированных профилей на уровне операционной системы Android и формировании обобщенных сведений, закладываемых в алгоритм осмотра мобильных средств связи; частнонаучные – для анализа эмпирического материала, а также в целях выявления технических и криминалистических особенностей, которые могут использоваться в различных архитектурах изолированных сред мобильных устройств. Результаты: предложен криминалистический алгоритм осмотра изолированных профилей мобильных устройств, включающий выявление признаков наличия «второго пространства», а также порядок фиксации цифровых доказательств.

Abstract. When investigating cybercrimes and other criminal acts committed via information and telecommunication technologies, investigators often need to examine mobile devices. However, the presence of a “second space” feature (a hidden, isolated user profile) can lead to the loss of critical digital evidence. The practical significance of this study lies in identifying data isolation mechanisms implemented by leading mobile device manufacturers (e.g., Samsung Secure Folder, MIUI (Xiaomi) Second Space, and Magic UI Private Mode (Huawei/Honor)). The purpose of this study is to examine the specifics of detecting and examining hidden workspaces in mobile devices actively exploited by criminals for illicit goals. The research employed a combination of general (description, generalization, and comparison), general scientific (analysis, synthesis), and specific scientific (cybernetic, systems analysis, and comparative legal) methods of cognition. General and general scientific methods were used to examine the technical architecture of isolated profiles within the Android OS and develop a generalized framework for mobile device forensic protocols. Meanwhile, specific scientific methods were applied to analyze empirical data and identify technical and forensic characteristics across various isolated environment architectures in mobile devices. Results: the study proposes forensic guidelines for examining isolated mobile device profiles, encompassing the detection of “second space” indicators and the procedure for securing digital evidence.

Ключевые слова: изолированный профиль, «второе пространство», цифровые доказательства, система Android, расследование киберпреступлений, криминалистика, изоляция данных, способы сокрытия цифровых следов, алгоритм осмотра, осмотр телефона

Для цитирования: Харисова З.И. Особенности осмотра изолированного профиля («второго пространства») мобильного средства связи при расследовании киберпреступлений / З.И. Харисова. – DOI 10.33184/pravgos-2026.3.13 // Правовое государство: теория и практика. – 2026. – № 3. – С. 110–118.

Keywords: isolated profile, second space, digital evidence, Android OS, cybercrime investigation, forensics, data isolation, anti-forensics techniques, forensic examination protocol, mobile device examination

For citation: Kharisova Z.I. Features of the Examination of the Isolated Profile ("Second Space") on Mobile Devices in Cybercrime Investigations. *The Rule-of-Law State: Theory and Practice*, 2026, no. 3, pp. 110–118. (In Russian). DOI 10.33184/pravgos-2026.3.13.

ВВЕДЕНИЕ

В структуре современной преступности наблюдается устойчивый рост деяний, совершаемых с использованием различных технических средств, преобладающей частью которых ввиду удобства эксплуатации являются мобильные устройства, зачастую выступающие в качестве инструмента связи, хранения данных или средства доступа к электронным средствам платежа.

Современные мобильные средства связи функционируют как сложные вычислительные устройства, обладающие возможностью создания изолированных пользовательских сред. Такие среды, как правило, реализуются в операционных системах семейства Android или HarmonyOS в виде специальных профилей – защищенных пространств, или «вторых пространств» (Second Space, Secure Folder, Private Space, Work Profile и др.)¹.

Функционал, изначально задуманный производителями для разделения личных и служебных данных, получил популярность у лиц, совершающих киберпреступления, как эффективный способ сокрытия цифровых следов. Как показывает анализ материалов уголовных дел о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий, изолированные пространства довольно часто используются профессиональными киберпреступниками для сокрытия противоправной деятельности,

в том числе хранения запрещенного контента, использования альтернативных (задействованных в преступной деятельности) аккаунтов в приложениях, запуска средств анонимизации, сокрытия криптографических ключей или мнемофраз от электронных кошельков. В этой связи исследование изолированных пользовательских профилей мобильных средств связи приобретает особую значимость.

ОБНАРУЖЕНИЕ СКРЫТЫХ РАБОЧИХ ПРОСТРАНСТВ В МОБИЛЬНЫХ СРЕДСТВАХ СВЯЗИ ПОД ОПЕРАЦИОННОЙ СИСТЕМОЙ ANDROID И ОСОБЕННОСТИ ОСМОТРА «ВТОРОГО ПРОСТРАНСТВА»

Следственный осмотр представляет собой непосредственное обнаружение и исследование объектов, имеющих значение для уголовного дела, их признаков, свойств, состояния и взаиморасположения [1, с. 528]. Основные цели следственного осмотра – обнаружение следов преступления и выяснение других обстоятельств, имеющих значение для расследования; к ним также можно отнести выявление и фиксацию признаков, которые в совокупности с имеющимися в уголовном деле данными могут служить основанием для признания предметов и документов вещественными доказательствами (ст. 176 УПК РФ).

В соответствии со ст. 177 УПК РФ осмотр мобильных средств связи должен осуществляться на месте производства следственного действия, однако если для осмотра требуется продолжительное время или осмотр на месте затруднен, осматриваемый объект упаковывается, опечатывается и заверяется подписью

¹ Исследование информации, содержащейся в мобильных телефонах : типовая методика / С.В. Ермолов, В.А. Рашупкина, Е.А. Кресан и др. М. : ЭКЦ МВД России, 2023. С. 10.

следователя. В дальнейшем его осмотр производится как самостоятельное следственное действие². На основании сведений, полученных в ходе осмотра, следователь может выдвинуть версии о характере преступления и его участниках, способе совершения и др. В связи с этим целесообразно рассмотреть особенности проведения осмотра современных мобильных средств связи, функционирующих под операционной системой Android, для обнаружения в них скрытых рабочих пространств, активно используемых преступниками в противоправных целях.

Анализ типовых методик проведения осмотра мобильных устройств позволяет говорить об их сугубо обобщенном характере, порой – устаревании, шаблонном подходе к такому устройству исключительно как к «предмету» или классически реализованному мобильному средству связи, а также о «разрыве» между реальной потребностью практики и изложением базовых и общеизвестных теоретических положений.

Мобильное устройство, на котором реализована функция «второго пространства», является довольно сложным объектом криминалистического исследования. На практике часто возникают ситуации, когда при беглом осмотре устройства (социальные сети, мессенджеры, фотографии) следователь не обнаруживает криминалистически значимых для расследования сведений, поскольку они располагаются в изолированной области памяти, доступ к которой защищен паролем, биометрическим «отпечатком» или вовсе скрыт программным путем. Криминалистическое исследование данных, расположенных во «втором пространстве», как правило, производится тем же набором средств и методов, которые используются при анализе основного пространства операционной системы мобильного устройства, но если осмотр основного профиля пользователя осуществляется по типовой методике проведения осмотра средства связи, то выявление и исследование изолированной среды требует существенно больших временных и интеллектуальных затрат.

² Справочник следователя : научно-методическое пособие (электронный формат). М. : ФГКУ «ВНИИ МВД России», 2023. Т. 1. С. 155 [Электронный ресурс]. URL: <https://media.mvd.ru/files/embed/4939086> (дата обращения: 01.04.2026).

Для разработки эффективной методики осмотра изолированных пользовательских профилей мобильных средств связи необходимо понимание технической реализации скрытых сред на уровне операционной системы устройства. Изолированные профили в мобильных средствах связи реализуются на уровне пользовательских пространств (User space), файловых систем (Sandboxing) или криптографической изоляции (Encryption keys per profile) [2, p. 180; 3, p. 470]. Например, в устройствах марки Samsung реализована аппаратно защищенная среда Knox Secure Folder [4, p. 74], в устройствах марки Xiaomi формируется отдельный пользователь с собственной файловой системой MIUI Second Space [5, p. 256], а в устройствах Huawei и Honor – изолированная среда Magic UI Private Space [6, p. 19].

Не останавливаясь подробно на особенностях разграничения прав доступа в мобильных операционных системах, необходимо отметить, что в основе функционала «второго пространства», как правило, лежит штатный механизм операционной системы семейства Android – многопользовательский режим Multiuser или профили с управляемыми привязками Managed Profiles; согласно документации Android Open Source Project (AOSP) каждому пользователю выделяется отдельная директория в каталоге устройства /data/user и собственное изолированное хранилище³. Приложения, установленные в изолированном профиле, не имеют доступа к данным основного пользователя, что позволяет программным путем «создать» два формально независимых устройства на одном физическом носителе. Данный факт подтверждается популярной современной практикой установки пользователями мобильных устройств во «второе пространство» приложений, функционирование которых по определенным причинам обязательно, но нежелательно с точки зрения обеспечения безопасности личных данных.

Криминалистически значимым при исследовании «второго пространства» мобильного устройства является то, что данные изолированного профиля не удаляются при сбросе настроек основного профиля и требуют

³ Операционная система с открытым исходным кодом «Android» (Open Source Project (AOSP)) [Электронный ресурс]. URL: <https://source.android.com/?hl=ru> (дата обращения: 25.03.2026).

отдельного форматирования раздела данных. Однако при стандартном подключении устройства к компьютеру, например, через режим МТР (от англ. media transfer protocol – протокол передачи мультимедиафайлов), пользователь видит только файлы активно-го в данный момент профиля.

Производители различных устройств внедряют собственные программные решения, которые модифицируют стандартную архитектуру операционной системы, что требует дифференцированного подхода к осмотру мобильных средств связи. Для эффективного выявления криминалистически значимых сведений при проведении осмотра устройств с целью обнаружения «второго пространства» необходимо владеть комплексом знаний и навыков, которые в ряде случаев могут обеспечить исследование (осмотр) мобильного средства связи без проведения экспертизы. Для этого необходимо различать модификации различных архитектур построения рассматриваемого функционала.

Так, например, для устройств марки Samsung (архитектура Knox Secure Folder) «второе пространство» создает изолированный контейнер на уровне ядра KNOX, шифруемый аппаратным ключом eSE. Данные внутри изолированной среды не видны при стандартном логическом извлечении без ввода пароля от скрытой папки или без использования специализированных криминалистических средств, способных обходить защиту ядра KNOX. Стоит также отметить, что в моделях устройств с операционной системой Android версии 13 и выше обход шифрования программными средствами, как правило, в настоящее время вообще невозможен.

Для устройств Xiaomi реализован полноценный второй пользовательский профиль, при этом переключение между пространствами осуществляется через меню «Настройки» или отдельный ярлык. Отличительной особенностью данных устройств является то, что файловая система «второго пространства» монтируется только при активном входе в него. При осмотре устройства, находящегося в «первом пространстве», данные «второго пространства» в общем хранилище не отображаются.

Для устройств Huawei и Honor реализация изолированного пространства максимально

схожа с MIUI Second Space от Xiaomi, но имеет особенность, связанную с возможностью полного сокрытия входа во «второе пространство» из настроек основного профиля, при этом для открытия скрытого профиля требуется ввод кода доступа в номеронабирателе или активация режима специально настроенным жестом.

Сам факт наличия изолированного профиля может быть установлен без доступа к его содержимому, для этого в ходе осмотра мобильного средства связи необходимо обращать внимание, например, на следующие цифровые «артефакты»:

- списки приложений App List, в которых могут фигурировать системные приложения или системные «менеджеры» изолированного пространства;

- файловая система с наличием, например, таких директорий, как /data/user/10 и т. п., если устройство было изъято в состоянии, позволяющем получить доступ к корневой файловой системе;

- логи установки Package Manager с записями о том, что приложение было установлено или запущено в профиле другого пользователя.

На практике выявление, равно как и осмотр «второго пространства», осложняется факторами, связанными с отсутствием явных признаков его наличия в интерфейсе устройства, скрытым режимом активации изолированной среды и маскировкой среды под системные функции. Косвенными признаками наличия «второго пространства» в ряде случаев могут выступать: наличие нескольких пользователей в системе, увеличенный объем занятой памяти на устройстве, наличие большого количества системных журналов (файлы logs), артефакты в файловой системе вида /data/system/users/ и т. п.

Основанием для производства осмотра мобильного средства связи является наличие у следователя достаточных данных о том, что в ходе процессуального действия будет получена информация, имеющая доказательственное значение для уголовного дела.

Осмотр мобильного средства связи проводится следователем, дознавателем, руководителем следственного органа либо органом дознания как по возбужденному уголовному делу, так и при проверке сообщения о преступлении, при этом понятые принимают участие

в данном следственном действии по усмотрению следователя (в отсутствие понятых применение технических средств фиксации хода и результатов следственного действия обязательно). Для участия в осмотре мобильного средства связи при необходимости может приглашаться лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, для постановки вопросов эксперту, а также для разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию (ст. 58 УПК РФ), – специалист. Зачастую именно от знания косвенных признаков наличия скрытых пространств в устройстве зависит необходимость приглашения специалиста, который в дальнейшем окажет помощь в обнаружении, фиксации и изъятии следов преступления, в том числе при выявлении скрытых «признаков» осматриваемого средства.

При проведении осмотра мобильного устройства необходимо строго соблюдать правила обращения с техническими средствами, учитывая перспективу их дальнейшего экспертного исследования [7, с. 78]. В некоторых случаях проводить осмотр средства связи допустимо только после проведения экспертизы, чтобы исключить возможность утраты информации или изменения свойств осматриваемого объекта.

Отдельной проблемой при проведении осмотра мобильных средств связи и изолированных пользовательских профилей мобильных устройств является установление или получение от владельца кода (пароля) как от основного, так и от «второго пространства». В судебной практике сложился условный подход, согласно которому отказ от предоставления кода доступа к телефону или изолированному профилю (если есть основания полагать, что там хранятся криминалистически значимые сведения) может расцениваться как воспрепятствование производству следственных действий [8, с. 96]. Однако следует помнить, что отказ в предоставлении следствию доступа к мобильному устройству не может считаться подтверждением вины его владельца, поскольку это нарушает презумпцию неви-

новности и конституционное право граждан на защиту своих прав и свобод (в виде правила *nemo tenetur* – права не свидетельствовать против себя)⁴ [9, с. 51]. В случае принятия за истину тезиса, что пароль – нейтральный ключ к доказательствам, попытка установить его не является истребованием цифровых данных. Таким образом, важно помнить, что обвиняемый защищен не только от непосредственно уличающих вопросов, он имеет более широкое право – на молчание [10, с. 70].

Если подозреваемый отказывается предоставить пароль, следователь не имеет права самостоятельно применять программные средства для подбора кода доступа, но вправе направить устройство на экспертизу, где эксперт, обладающий специальными знаниями и необходимыми программными средствами, может извлечь данные из изолированного профиля в рамках производства экспертизы. Если у следователя имеется пароль доступа к основному и (или) «второму пространству», можно руководствоваться следующим алгоритмом действий.

1. Перевести устройство связи в авиарежим для недопущения изменения текущего его состояния и удаленного уничтожения информации⁵.

2. Подключить устройство к сети питания (по возможности).

3. Установить (со слов задержанного либо иным способом) и внести в протокол пароль доступа к устройству.

4. Провести в присутствии понятых сброс парольной защиты для обеспечения дальнейшего свободного входа в мобильное устройство.

5. Проверить наличие на устройстве изолированных пользовательских профилей.

⁴ Определение Судебной коллегии по уголовным делам Верховного Суда РФ от 21.09.2023 № 16-УД23-17-К4; Приговор по ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ (покушение; незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов) // Доступ из справ.-правовой системы «КонсультантПлюс».

⁵ Рекомендации по взаимодействию органов предварительного следствия, оперативных и экспертно-криминалистических подразделений при необходимости экспертного исследования материалов, включающих интернет-переписку участников организованных групп, по уголовным делам, связанным с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров: методические рекомендации. М.: ЭКЦ МВД России; Следственный департамент МВД России; ГУНК МВД России, 2020. С. 17.

6. Выявить признаки наличия изолированного пользовательского профиля на мобильном средстве связи навигацией в меню настроек операционной системы.

6.1. Проверить в меню «Настройки», пункт «Пользователи и аккаунты», наличие записей «Гость», «Второе пространство» или «Безопасная папка», проверить список установленных приложений на наличие разделов Secure Folder, Second Space, Parallel Space, Shelter и т. п., а также шторки уведомлений на наличие иконки переключения профилей пользователей.

6.2. Извлечь информацию (если изолированный профиль активен (например, устройство находится в «безопасной папке» при изъятии) или подозреваемый добровольно предоставил доступ – производится фото- или видеосъемка содержимого), зафиксировать приложения внутри изолированного профиля.

6.3. Составить перечень файлов, расположенных в загрузках, галерее, данных в телефонной книге и прочих криминалистически значимых сведений.

7. Проверить сервисы и мессенджеры, функционирующие на момент осмотра, отключить в настройках функцию автоматического удаления сообщений (при обнаружении защищенных паролем сервисов и мессенджеров установить пароль и внести его в протокол).

8. Зафиксировать переписку и другую значимую информацию путем создания снимков экрана или фотосъемки изображений на экране осматриваемого устройства.

9. Проверить историю установленных на устройстве браузеров в целях определения посещаемых веб-ресурсов.

10. При выявлении запрещенных веб-ресурсов установить и зафиксировать в протоколе пользовательские учетные данные для доступа к ним.

11. Проверить устройство на наличие программного обеспечения, способного отслеживать действия пользователя, в случае обнаружения принять меры для его отключения.

12. Осмотреть перечень программного обеспечения, фиксирующего заметки пользователя, календари, ежедневники, файлы и документы на наличие в них учетных данных, а также другой значимой информации.

13. Проверить хранилище графических изображений на наличие фотоизображений,

а также иной информации, позволяющей изобличить преступника.

14. По результатам осмотра составить протокол осмотра предмета (мобильного средства связи) с приложением фототаблиц.

15. В случае невозможности извлечения данных из-за блокировки устройства вынести постановление о назначении компьютерно-технической экспертизы.

При описании внешнего вида телефона в протоколе осмотра следует отразить: наименование, марку, размеры, цвет, конструкцию, материал, из которого изготовлено устройство; модель и ее характеристики; фоновый рисунок или иные особенности визуального отображения; имя владельца на дисплее; наличие повреждений; наличие изолированных пользовательских профилей [11, с. 47].

В ходе проведения осмотра мобильного средства связи следует также установить:

- уникальный IMEI-код (от англ. international mobile equipment identity – международный идентификатор мобильного оборудования) средства связи путем набора на мобильном устройстве комбинации *#06# [12, с. 23];

- абонентский номер, идентифицирующий элемент сети связи, путем набора комбинации клавиш, определенной оператором связи;

- информацию о соединениях между абонентскими устройствами, например, путем создания личного кабинета пользователя, использования приложения от оператора связи либо веб-версии личного кабинета абонента с целью извлечения детализации разговоров и обмена сообщениями (с письменного согласия владельца);

- данные об IP-адресе и MAC-идентификаторе, количестве слотов для SIM-карты, видах операторов, определенных устройством, и IMEI-кодах путем детального осмотра технического средства встроенными средствами операционной системы;

- сохраненные данные о беспроводных устройствах и подключениях (в разделе расширенных свойств имеются данные о MAC-адресе устройства, с которого осуществлялась раздача, и выделенный IP-адрес);

- данные об аккаунте и привязанных банковских картах, в том числе виртуальных электронных кошельках (в приложениях, мессенджерах).

Установленный IMEI-код сразу же в ходе осмотра можно проверить путем использования специальных сервисов (например, на сайте <https://www.imei.info>)⁶. Широкий спектр возможностей позволяет не только удостовериться в действительности IMEI-кода технического средства без постороннего вмешательства в программное обеспечение, но и перепроверить в базах данных информацию о его утере или хищении. Полученная информация отражается в протоколе с описанием процедуры получения сведений.

Информация о соединениях между абонентами может быть получена в ходе как осмотра сотового телефона путем использования подключенного личного кабинета, так и направления запроса оператору связи. При направлении запроса следует требовать информацию о базовых станциях с указанием азимутов обслуживания абонента. Кроме того, возможно использование сайтов, позволяющих установить координаты базовых станций, определить с помощью карт, размещенных в сети Интернет, местонахождение абонента.

Представленный порядок осмотра мобильных устройств с отражением особенностей выявления и исследования изолированных пользовательских профилей имеет прикладное значение для практики расследования киберпреступлений, обеспечивая преодоление разрыва между техническими возможностями сокрытия криминалистически значимой информации и механизмами ее поиска, фиксации, извлечения, исследования и проверки, позволяя в ряде случаев подтвердить факт наличия скрытого раздела памяти еще до получения доступа к его содержимому.

Стоит обратить особое внимание на то, что мобильные устройства под управлением операционной системы Android популярны у лиц, совершающих киберпреступления, что имеет определенные основания, которые необходимо учитывать при разработке криминалистических методик расследования указанных преступных деяний.

Привлекательность любой технологической платформы для киберпреступников определяется рядом факторов, например, рас-

пространенностью ее использования, средствами или возможностями, предоставляемыми данной платформой. Операционная система Android – единственная мобильная программная оболочка, в которой указанные факторы достигают уровня, сопоставимого с экосистемой Windows от Microsoft, позволяющей гибко настраивать программные средства под конкретные нужды пользователя и варьировать установкой сборок (прошивок или кастомных версий программного обеспечения), ориентированных на обеспечение анонимности в сети Интернет.

Мотив киберпреступников при выборе мобильных средств под управлением системы Android для использования в противоправной деятельности обусловлен масштабом пользовательской базы. По официальным статистическим данным сервиса веб-аналитики StatCounter, устройства на базе Android занимают доминирующее положение на мировом рынке мобильных устройств (более 68 % от общего объема мобильных систем)⁷, что создает сравнительно большую выборку доступных для эксплуатации устройств.

Кроме того, в системе Android представлен широкий арсенал программируемых средств, который может использоваться киберпреступниками, что обусловлено архитектурными особенностями программной оболочки, в частности открытостью экосистемы (в отличие от системы iOS, где распространение приложений контролируется через магазин приложений App Store с обязательной верификацией личности разработчика, система Android позволяет устанавливать программное обеспечение из любых источников). Наличие таких преимуществ, в частности инструментов клонирования и изоляции рабочих пространств и разделения учетных записей в системе Android, активно используется преступниками для создания защищенных сред в противоправных целях.

ЗАКЛЮЧЕНИЕ

Предложенный криминалистический алгоритм осмотра мобильных средств связи с

⁶ Сервис проверки IMEI-номеров мобильных средств связи [Электронный ресурс]. URL: <https://www.imei.info> (дата обращения: 25.03.2026).

⁷ Mobile Operating System Market Share Worldwide (February 2026) [Электронный ресурс]. URL: <https://gs.statcounter.com/os-market-share/mobile/worldwide> (дата обращения: 25.03.2026).

отражением возможности выявления и осмотра изолированных профилей представляет собой своеобразный «отклик» на комплекс вызовов, порожденных архитектурными особенностями преобладающей в настоящее время в технических средствах киберпреступников операционной системы Android.

Прикладное значение исследования заключается в возможности использования адаптированного под нужды практики алгоритма действий при обнаружении признаков наличия изолированного профиля в мобильном средстве связи, включающего фиксацию факта «второго пространства» и порядок действий по его осмотру.

С развитием мобильных операционных систем и внедрением аппаратных модулей защиты классические методы логического извлечения данных [13, с. 120] становятся менее эффективными, кроме того, в обозримом будущем прогнозируется увеличение доли устройств, где изолированные профили будут защищены специальными чипами безопасности eSE [14, р. 301928], не поддающимися программному обходу даже в условиях экспертного исследования.

Таким образом, можно сделать вывод, что изолированные профили мобильных средств связи, представляя собой довольно сложные объекты для криминалистического исследования, требуют от следователя и специалиста не только знания порядка проведения осмотра основного пространства мобильного устройства или процессуальных особенностей фиксации, изъятия или исследования цифровых следов из защищенных контейнеров без нарушения целостности доказательственной информации, но и понимания процессуальных границ допустимого вмешательства, владения знаниями о файловой системе и архитектуре операционной системы Android, принципов их функционирования, механизмов шифрования данных внутри изолированных сред, методов их обнаружения и «обхода» программных барьеров. Соответственно, разработанный алгоритм осмотра мобильных средств связи с функцией изолированных пользовательских профилей является одним из составных элементов системы противодействия киберпреступности в условиях доминирования на рынке Android-устройств.

СПИСОК ИСТОЧНИКОВ

1. Криминалистика : учебник / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская. – Москва : Норма: ИНФРА-М, 2026. – 928 с.
2. Tiwari M. Technical Challenges of Encryption in Mobile Forensics / M. Tiwari, S. Thapaliya // *International Journal of Multidisciplinary and Innovative Research*. – 2025. – Vol. 12 (6). – P. 178–183.
3. Patel B. A Survey on Mobile Digital Forensic: Taxonomy, Tools, and Challenges / B. Patel, P. Mann // *Security and Privacy*. – 2025. – Vol. 8 (2). – P. 470–478.
4. Heasley J.S. Anti-forensics for Mobile Devices: Exploring Apps Encountered by Digital Forensic Investigators: diss. Master of Science degree / J.S. Heasley. – West Lafayette (Purdue University Graduate School), 2025. – 107 p.
5. Fakhriansyah A. Development of Xiaomi Product Mobile Forensic Acquisition Framework on Second Space Features Based on SNI/ISO 27037:2014 / A. Fakhriansyah, A. Luthfi // *Jurnal Infotel*. – 2024. – Vol. 16 (2). – P. 255–272.
6. Liu H. Safeguarding user security and privacy: seeing through communications and obfuscating network activities: diss. Doctor of Philosophy degree / H.Liu. – Edinburgh (Institute of Computing Systems Architecture), 2023. – 197 p.

REFERENCES

1. Averianova T.V., Belkin R.S., Korukhov Yu.G., Rossinskaya E.R. Forensic Science. Moscow, Norma: INFRA-M Publ., 2026. 928 p.
2. Tiwari M., Thapaliya S. Technical Challenges of Encryption in Mobile Forensics. *International Journal of Multidisciplinary and Innovative Research*, 2025, vol. 12 (6), pp. 178–183. (In English).
3. Patel B., Mann P. A Survey on Mobile Digital Forensic: Taxonomy, Tools, and Challenges. *Security and Privacy*, 2025, vol. 8 (2), pp. 470–478. (In English).
4. Heasley J.S. Anti-forensics for Mobile Devices: Exploring Apps Encountered by Digital Forensic Investigators. *Master Diss.* West Lafayette (Purdue University Graduate School), 2025. 107 p.
5. Fakhriansyah A., Luthfi A. Development of Xiaomi Product Mobile Forensic Acquisition Framework on Second Space Features Based on SNI/ISO 27037:2014. *Jurnal Infotel*, 2024, vol. 16(2), pp. 255–272. (In English).
6. Liu H. Safeguarding User Security and Privacy: Seeing Through Communications and Obfuscating Network Activities. *Doct. Diss.* Edinburgh (Institute of Computing Systems Architecture), 2023. 197 p.

7. Максимович А.Б. Средства сотовой связи как объект криминалистического исследования : дис. ... канд. юрид. наук : 12.00.12 / А.Б. Максимович. – Москва, 2018. – 251 с.

8. Скобелин С. Ю. Возможности получения криминалистически значимой информации при осмотре мобильных средств связи и пределы ограничения конституционных прав граждан на тайну переписки / С. Ю. Скобелин // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2017. – № 1. – С. 89–98.

9. Третьякова Е.И. Мобильный телефон как источник криминалистически значимой информации / Е.И. Третьякова // Вестник Уральского финансово-юридического института. – 2018. – № 3 (13). – С. 49–51.

10. Коновалов С.Г. Содействие обвиняемого в разблокировке его смартфона: допустимо ли принуждение? / С.Г. Коновалов // Закон. – 2025. – № 2. – С. 69–80.

11. Особенности проведения проверки сообщений о преступлениях, совершаемых с использованием информационно-телекоммуникационных технологий / В.С. Латыпов, Э.Д. Нугаева, З.И. Харисова, Т.С. Соколова. – Москва : Мир науки, 2026. – 85 с.

12. Расследование мошенничеств, совершаемых с использованием мобильной связи : учебное пособие / О.П. Грибунов, М.В. Старичков, А.А. Шаевич и др. – Иркутск : Восточно-Сибирский институт Министерства внутренних дел РФ, 2018. – 44 с.

13. Головчанский А.В. Техничко-криминалистическое обеспечение производства следственных действий, связанных с изъятием и осмотром мобильных средств сотовой связи / А.В. Головчанский // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. – 2015. – № 1. – С. 118–123.

14. Song S. Forensic recovery via chip-transplantation in Samsung smartphones / S. Song, Y. Hongseok, E. Lee // Forensic Science International: Digital Investigation. – 2025. – Vol. 53 (1). – P. 301926–301936.

7. Maksimovich A.B. Cellular Communication Equipment as an Object of Forensic Research. *Cand. Diss.* Moscow, 2018. 251 p.

8. Skobelin S.Yu. The Possibility of Obtaining a Forensically Relevant Information During the Inspection of Mobile Communication Devices of Participants of Criminal Proceedings and Limits of Constitutional Rights of Citizens to Privacy of Correspondence. *Crime in the Sphere of Information and Telecommunication Technologies: Problems of Prevention, Detection, and Investigation of Crimes*, 2017, no. 1, pp. 89–98. (In Russian).

9. Tretyakova E.I. Mobile Phone as a Source of Forensically Significant Information. *Bulletin of the Ural Financial and Law Institute*, 2018, no. 3 (13), pp. 49–51. (In Russian).

10. Konovalov S.G. Assistance of the Accused in Unlocking His Smartphone: Is Coercion Acceptable? *Zakon*, 2025, no. 2, pp. 69–80. (In Russian).

11. Latypov V.S., Nugaeva E.D., Kharisova Z.I., Sokolova T.S. Features of the Verification of Reports of Crimes Committed Using Information and Telecommunication Technologies. Moscow, Mir nauki Publ., 2026. 85 p.

12. Gribunov O.P., Starichkov M.V., Shaevich A.A. et al. Investigation of Fraud Committed Using Mobile Communications. East Siberian Institute of the Ministry of Internal Affairs of the Russian Federation Publ., 2018. 44 p.

13. Golovchansky A.V. Technical and Forensic Support for Investigative Actions Related to the Seizure and Inspection of Mobile Cellular Devices. *Crime in the Field of Information and Telecommunication Technologies: Problems of Prevention, Detection and Investigation of Crimes*, 2015, no. 1, pp. 118–123. (In Russian).

14. Song S., Hongseok Y., Lee E. Forensic Recovery Via Chip-Transplantation in Samsung Smartphones. *Forensic Science International: Digital Investigation*, 2025, vol. 53 (1), pp. 301926–301936. (In English).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Харисова Зарина Ирековна – доктор юридических наук, кандидат технических наук, доцент, доцент кафедры криминалистики Института права.

INFORMATION ABOUT THE AUTHOR

Kharisova Zarina Irekovna – Doctor of Sciences (Law), Candidate of Technical Sciences, Associate Professor of the Department of Criminalistics, Institute of Law.

Статья поступила в редакцию 01.04.2026; одобрена после рецензирования 30.04.2026; принята к публикации 30.04.2026. The article was submitted 01.04.2026; approved after reviewing 30.04.2026; accepted for publication 30.04.2026.