Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Some aspects of mobile device research: Uzbekistan's experience

Hagani GAJIYEV[1], Azizbek XUDOYBERDIYEV [2]

Main Forensic Center of the Ministry of Internal Affairs

ARTICLE INFO

Article history:
Received September 2020
Received in revised form
15 November 2020
Accepted 20 November 2020
Available online
15 December 2020

Keywords:
Forensic science
Mobile device research
Mobile forensics
Obtaining digital evidence.

ABSTRACT

The article highlights the importance of forensic research of mobile devices in the period of intensive digitalization of modern society. The author explores innovative approaches to obtaining digital evidence from mobile devices, analyzes the legal framework in this area, and develops scientific-practical proposals and recommendations.

Мобил қурилмаларни тадқиқ этишнинг айрим аспектлари: Ўзбекистон тажрибасида

Калит сўзлар:
Форензика
Мобил қурилмалар тадқиқоти
Мобил алоқа воситалари криминалистикаси
Рақамли далилларни олиш

АННОТАЦИЯ

Ушбу мақолада замонавий жамиятни жадал рақамлаштириш даврида мобил қурилмаларни суд-техник экспертизасининг аҳамияти келтирилган. Мазкур мақолада муаллиф томонидан мобил қурилмалардан рақамли далилларни олишнинг инновацион ёндашувлари ўрганилган, ушбу соҳадаги меъёрий-ҳуқуқий база таҳлил қилинган, шунингдек илмий ва амалий таклифлар ҳамда тавсиялар ишлаб чиқилган.

[1] Main Forensic Center of the Ministry of Internal Affairs of the Republic of Uzbekistan
E-mail: axagani89@gmail.com
[2] Main Forensic Center of the Ministry of Internal Affairs of the Republic of Uzbekistan
E-mail: b xucking1991@gmail.com

Некоторые аспекты исследования мобильных устройств: опыт Узбекистана

Ключевые слова:
Форензика
Исследование мобильных устройств
Мобильная криминалистика
Получение цифровых доказательств

АННОТАЦИЯ

В статье освещается значимость криминалистического исследования мобильных устройств в период интенсивной цифровизации современного общества. Автором исследуются инновационные подходы получения цифровых доказательств из мобильных устройств, анализируется нормативно-правовая база в данной сфере, а также разрабатываются научно-практические предложения и рекомендации.

ВВЕДЕНИЕ

В Постановлении Президента Республики Узбекистан №-4024 «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты» от 21 ноября 2018 г. отмечено, что внедрение современных информационно-коммуникационных систем в сфере государственного и общественного управления является важным условием эффективной реализации проводимых социально-экономических и общественно-политических реформ и преобразований в стране. [1]

В системе мер по нейтрализации и искоренению преступности, наиболее действенными в настоящее время являются информационные технологии, позволяющие использовать при раскрытии и расследовании преступлений самые современные достижения науки и техники. [2]

Период активного внедрения цифровых технологий во все сферы деятельности современного общества обусловливает актуальность исследования компьютерной техники и мобильных устройств. Заключение экспертизы мобильных устройств и компьютерно-технической экспертизы является одним из основных источников доказательств в ходе расследования преступлений, сопряженных с применением компьютерных средств. В связи с постоянным и быстрым развитием информационных технологий данный вид исследований считается одним из сложных.

Несмотря на тот факт, что мобильные устройства, в частности сотовые телефоны, используются при совершении преступлений достаточно давно, криминалистический анализ данных, которые они содержат, является сравнительно молодым направлением компьютерной криминалистики или «форензики» [3], появившемся лишь в начале 2000-х. Такое ответвление обусловлено тем, что традиционные методы форензики не могли быть применены ко многим мобильным устройствам, что обусловило необходимость разработки новых методик для их исследования. [4]

Таким образом, если форензика – это «прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств» [3], то криминалистическое исследование мобильных устройств или мобильная

криминалистика – подраздел форензики, занимающийся поиском, извлечением и фиксацией цифровых доказательств, имеющихся в мобильных устройствах, таких как сотовые телефоны, смартфоны, планшетные компьютеры и т.п.

Анализ практики свидетельствует о том, что основное количество цифровых носителей информации, поступающих *лабораторию цифровых экспертиз,* Главного экспертно-криминалистического центра МВД Республики Узбекистан составляют именно мобильные устройства. Наблюдаются высокие показатели проведения исследований мобильных устройств (более 75% за период 9 месяцев 2019 года от общего числа поступивших объектов и более 85% за период 9 месяцев 2020 года).

Изложенное определяет *актуальность* нашего исследования.

В нашем исследовании мы будем рассматривать этапы проведения исследования мобильных устройств ипроцессы получения цифровых доказательств.

Научная новизна исследования представлена анализом современных методов и уровней извлечения данных с мобильных устройств.

Целью исследования является анализсовременных комплексов и программных обеспечений которые наиболее эффективны в проведении исследований в области мобильной криминалистики – подраздела форензики учитывая потребительский рынок Республики Узбекистан в использовании мобильных телефонов.

МАТЕРИАЛЫ И МЕТОДЫ

В год поддержки активного предпринимательства, инновационных идей и технологий в 2018 г., в структуре Главного экспертно-криминалистического центра МВД Республики Узбекистан (далее – ГЭКЦ), было образовано «Отделение внедрения и развития ИКТ» основной задачей которого является проведение исследований в области компьютерно-технической экспертизы и мобильных устройств.

Со стороны профильных специалистов ГЭКЦ были изучены новейшие инновационные технологии исследования мобильных устройств при содействии председательства Корейского агентства по международному сотрудничеству KOICA на базе Национального центра цифровой экспертизы Генеральной прокуратуры Республики Корея. После чего в судебно-экспертную практику ГЭКЦ первые были внедрены программные обеспечения корейских производителей Final Mobile Forensic, Hancom GMD по восстановлению, извлечению и анализу информации с сотовых телефонов и мобильных устройств.

Согласно Постановления Кабинета Министров Республики Узбекистан от 14 августа 2017 года №626 «О мерах по укреплению материально-технической базы органов внутренних дел Республики Узбекистан» и Программы поэтапного оснащения на период 2017-2021 годы, были произведены закупки универсальных аппаратно-программных комплексов для криминалистических исследований цифровых носителей информации и мобильных устройств Cellebrite UFED, дающие возможность извлекать, декодировать и анализировать цифровые данные, полученные из мобильных устройств.

В ГЭКЦ проводятся исследования объектов компьютерно-технической экспертизы и мобильных устройств, апробированы современные методы

извлечения данных с мобильных телефонов. Кроме того, были разработаны методические рекомендации для экспертов по производству судебно-компьютерно-технических экспертиз, одобренные Ученым советом Республиканского центра судебной экспертизы им. Х. Сулаймановой при Министерстве Юстиции Республики Узбекистан (Протокол №01/20 от 17 января 2020 г.), а после включены в Реестр судебно-экспертных методик.

В связи с созданием двухсторонних отношений между Республикой Узбекистан и Республикой Корея и достигнутыми договорённостями в рамках государственного визита президента Республики Корея Мун ЧжэИна в апреле 2019 года, были обсуждены перспективы взаимодействия в различных направлениях сотрудничества, в том числе в сфере противодействия преступности. [5]

Благодаря достигнутым договорённостям 2021 г. запланировано заключение Меморандума о сотрудничестве в области цифровой криминалистики между ГЭКЦ МВД Республики Узбекистан и Национальным центром цифровых экспертиз (NDFC) Генеральной прокуратуры Республики Корея, что в свою очередь позволит расширить сотрудничество в совместной научной деятельности в области цифровой криминалистики. Это сотрудничество будет включать совместные проекты, краткосрочные визиты по обмену опытом и долгосрочные визиты для проведения совместных исследований.

Взаимовыгодное сотрудничество и внедрение указанных инновационных технологий позволило реализовать планы по дальнейшему внедрению и усовершенствованию цифровых экспертиз в ГЭКЦ МВД Республики Узбекистан, обеспечить современное техническое оснащения экспертных подразделений, получить возможности извлечения данных на физическом уровне и декодирование полученных данных с обходом блокировки вводом графического ключа / пароля / PIN-кода с устройств Android и другие, производить извлечение на уровне файловой системы из любых устройств Windows Phone, HTC, Samsung, Huawei и ZTE, осуществить возможность дешифрования зашифрованной базы данных истории WhatsApp, получить богатый выбор вариантов декодирования: данные приложений, пароли, электронная почта, журнал вызовов, SMS, контакты, календарь, мультимедийные файлы, информация о расположении и т.п. [6]

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЯ

Представленные нами возможности в проведении исследований мобильных устройств это лишь часть того что, имеет большую востребованность и интерес для органов следствия и дознания в расследовании преступлений.

Однако, не все категории данных, даже при условии наличия их в мобильном устройстве, доступны для извлечения. Прежде всего, это связано с аппаратными и программными особенностями хранения данных в конкретном мобильном устройстве.

В связи с чем необходимо рассмотреть современные аппаратно-программные комплексы и программные обеспечения, широко применяемые на сегодняшний день в практической деятельности экспертов криминалистов в производстве исследований мобильных устройств.

Широкий спектр по решению вопросов исследования мобильных устройств предлагают такие компании как Cellebrite UFED, Final Data (final mobile forensic),

HANCOM GMD (md next, md read), XRAY, Oxygen Forensic (Мобильный криминалист), Meya Pico, Elcomsoft и др.

Исходя из опыта применения в практической деятельности некоторых выше указанных комплексов и программных обеспечений были выявлены проблемы, связанные с тем, что некоторые заявленные возможности не соответствовали действительности при выполнении определенных поставленных задач перед экспертами.

Рассмотрим на примере универсального аппаратно-программного комплекса UFED 4PC. Данный комплекс предназначен для криминалистических исследований, дающий возможность извлекать, декодировать и анализировать цифровые данные, полученные из мобильных устройств, на существующем ПК или ноутбуке. [6]

Комплекс позволяет осуществить доступ к десяткам тысяч мобильных устройств, не сложен в применении, имеет хороший интерфейс, не требует постоянной технической поддержки. UFED Physical Analyzer производит обработку и анализ данных в реальном времени, создает соответствующие требованиям отчеты, которые можно приобщить к заключению эксперта и материалам уголовного дела.

Программные обеспечения корейских производителей Final Data (final mobile forensic), HANCOM GMD (md next, md read) имеют очень широкий спектр возможностей в решении задач в исследовании мобильных устройств. Положительно оценивается извлечение данных с их помощью с мобильных телефонов Samsung, LG, Sky, Huawei, и др., отлично производится обработка и анализ данных с возможностью проигрывания восстановленных файлов с графическими изображениями и аудиовизуальными данными.

Отрицательными сторонами данных ПО является то, что список поддержки большинства мобильных устройств содержит модели телефонов, распространённых на корейском рынке. В Республике Корея используются брендовые и иные модели телефонов, отличающиеся от экспортных вариантов, которые широко распространены в Узбекистане. По этой причине периодически приходится пользоваться технической поддержкой специалистов корейской компании.

Перед тем, как перейти к особенностям получения цифровых доказательств из мобильных устройств необходимо рассмотреть основополагающие принципы сбора цифровых доказательств.

В большинстве юрисдикций и организаций цифровые доказательства обусловлены тремя основополагающими принципами: значимость, достоверность и достаточность. [7]

-значимость, заключается в том, что должна быть возможна демонстрация значимости для расследования полученного материала, т.е. он содержит ценную информацию для содействия расследованию конкретного инцидента и существует достаточное основание для его получения. Для проверки и обоснованности **специалист** должен описать соблюдаемые процедуры и объяснить, как было принято решение о получении каждого элемента;

-достоверность обозначает контролируемость и повторяемость всех процессов, используемых при обращении с потенциальными цифровыми

доказательствами. Результаты применения таких процессов должны быть воспроизводимыми;

-достаточность обеспечивает необходимое количество данных, чтобы сделать возможным проведение надлежащего расследования. Для проверки и обоснованности специалист должен указать, сколько данных в совокупности рассматривалось, и какие процедуры использовались для принятия решения о том, сколько и какие данные нужно получить.

Информация может быть собрана путем получения доказательств и/или осуществления мероприятий по сбору.

Анализ имеющейся научной литературы показал, что процесс получения цифровых доказательств из мобильных устройств включает семь стадий: [8]

1. ***Представление объекта на экспертизу***. На данном этапе следственным органом (органом дознания, судом) готовится постановление о назначении компьютерной (компьютерно-технической) экспертизы, которое впоследствии поступает в экспертное учреждение вместе с объектом исследования. Необходимо отметить важность предварительного согласования вопросов, ставящихся на разрешение эксперту, последним. Кроме того, необходимо удостовериться в отсутствии повреждений упаковки объекта, а также соответствии представляемых на экспертизу объектов тем, что указаны в постановлении о назначении экспертизы.

2. ***Идентификация объекта.*** Эксперт, которому поручено производство экспертизы, предварительно сфотографировав упаковку, извлекает из нее поступивший на исследование объект. Производится сопоставление извлеченного из пакета устройства с устройством, указанным в постановлении о назначении экспертизы. Фиксируется производитель, модель и серийный номер устройства, IMEI, а также иные особенности его индивидуализирующие (цвет, тип корпуса, повреждения и т.п.). Устанавливается наличие в корпусе мобильного устройства SIM-карт и карт памяти.

3. ***Подготовка к исследованию.*** Необходимая для этой стадии информация уже собрана экспертом при идентификации объекта. Получив сведения о производителе и модели, криминалист может найти и изучить документацию на устройство, подобрать соответствующий кабель, программное обеспечение, необходимое для проведения исследования, в том числе драйверы, необходимые для взаимодействия мобильного устройства с рабочей станцией эксперта. При выборе программного обеспечения необходимо руководствоваться задачами исследования, ресурсами, находящимися в распоряжении экспертно-криминалистического подразделения, типом мобильного устройства, а также наличием в нем сменных носителей информации.

4. ***Изоляция объекта.*** Большинство мобильных устройств взаимодействуют с сетями сотовой связи и иными через «Bluetooth», ИК-порт и Wi-Fi-модуль. На данной стадии эксперт изолирует устройство от всех этих сетей. Это позволяет избежать внесения изменений в данные, имеющиеся в памяти устройства, например, входящими вызовами, SMS-сообщениями и т.п. Кроме того, некоторые устройства поддерживают удаленный доступ, воспользовавшись которым подозреваемый может уничтожить цифровые доказательства. Для этих целей может быть использована, например, клетка Фарадея, которая экранирует

устройство от внешних электромагнитных полей. Кроме того, большинство смартфонов и планшетных компьютеров имеют встроенный режим «В самолете», который также позволяет отключить устройство от всех сетей.

Использование клетки Фарадея (устройство для экранирования аппаратуры от внешних электромагнитных полей) или иной упаковки с экранированием излучений радиочастот может усилить истощение аккумулятора телефона мобильной связи. Это может потребовать обеспечения резервного питания для находящегося в упаковке устройства, если позволяют ресурсы. [7]

5. ***Извлечение данных.*** Изолировав мобильное устройство от сетей, эксперт приступает к непосредственному извлечению и анализу данных посредством избранного программного обеспечения (и аппаратно-программных комплексов). Необходимо отметить, что внешние носители информации (карты памяти) должны исследоваться отдельно, так как существует вероятность внесения изменений в данные, хранящиеся на ней, во время исследования мобильного устройства. При исследовании карт памяти необходимо применять традиционные методы компьютерной криминалистики, которые позволяют сохранить исследуемую компьютерную информацию в первозданном виде.

Остановимся более подробно на уровнях извлечения данных, обратившись к книге «Практическая мобильная криминалистика». [9] Итак, существует пять основных уровней извлечения данных из мобильных устройств, каждый из которых имеет свои недостатки и преимущества. Данные уровни были представлены Сэмом Бразерсом, в 2009 году, в виде пирамиды [10], по мере приближения к вершине которой методы становятся более сложными с технической стороны, правильными с точки зрения криминалистики и наукоемкими. Пирамида, иллюстрирующая все пять уровней извлечения данных из мобильных устройств представлена на рисунке №1.

Рисунок 1. Уровни извлечения данных из мобильных устройств

Ручное извлечение данных. Данный уровень подразумевает обеспечение доступа к компьютерной информации, имеющейся в памяти мобильного устройства, посредством его клавиатуры или сенсорного экрана. Обнаруженная в ходе исследования информация документируется путем фотосъемки экрана телефона или планшета. Данные метод является наиболее простым и подходит для любого устройства. Важно отметить, что на данном уровне невозможно получить все данные, а также произвести восстановление удаленных файлов и записей. Несмотря на кажущуюся простоту данного метода, некоторые типы данных (например, сведения об электронной почте, хранимой в мобильном устройстве фирмы Apple), возможно получить только данным способом.

Извлечение данных на логическом уровне. Данный уровень подразумевает подключение мобильного устройства к рабочей станции эксперта посредством USB-кабеля, ИК-порта или «Bluetooth». После этого производится побитовое копирование файлов и каталогов, находящихся на логических дисках мобильного устройства. При этом используется интерфейс прикладного программирования, разработанный производителем и предназначенный для синхронизации телефона или планшета с персональным компьютером. Тем не менее, данный уровень извлечения данных также обеспечивает ограниченный доступ к компьютерной информации, и не позволяет восстановить удаленные данные. Исключением могут служить удаленные записи из баз данных SQLite, использование которых характерно для операционных систем iOS и Android. Стертые записи в указанных базах данных не перезаписываются сразу, а помечаются как «удаленные» до тех пор, пока место, занимаемое ими, не понадобится для записи новых данных. Также, на этом уровне возможно извлечение баз миниатюр, содержащих миниатюры графических и видео файлов, содержащихся в устройстве, в том числе, и удаленных файлов данных типов.

Извлечение данных на физическом уровне. Этот уровень подразумевает получение побитовой копии всей внутренней памяти мобильного устройства, что позволяет, в том числе, восстановить удаленные записи и файлы. Несмотря на привлекательность данного метода, осуществить извлечение данных на этом уровне представляется возможным далеко не всегда: производители зачастую ограничивают возможность чтения внутренней памяти мобильного устройства в целях обеспечения максимальной безопасности. Чтобы обойти данные ограничения, разработчики программного обеспечения для криминалистического исследования мобильных устройств разрабатывают собственные загрузчики, которые позволяют не только получить доступ к внутренней памяти, но и, иногда, обойти пароли, установленные пользователями.

Извлечение данных из интегральной схемы памяти или «Chip-off». Данный уровень подразумевает извлечение данных непосредственно из интегральной схемы памяти мобильного устройства. Интегральная схема извлекается из телефона или планшета и помещается в соответствующее устройство для чтения или аналогичное мобильное устройство. Использовать данный метод достаточно сложно, так как интегральные схемы памяти, используемые в производстве мобильных устройств, весьма разнообразны. Преимуществом же извлечения данных на этом уровне является возможность получить компьютерную информацию даже из памяти неисправных мобильных устройств.

Отдельного внимания заслуживает метод извлечения данных из интегральной схемы памяти посредством отладочного интерфейса JTAG (Joint Test Action Group). Устройство подключается через порт тестирования (TAP) и его процессор получает команду на копирование данных, имеющихся на интегральной схеме памяти.

Извлечение данных на микроуровне. Данный процесс подразумевает изучение интегральной схемы памяти посредством электронного микроскопа и последующее преобразование полученных данных сначала в последовательность нулей и единиц, затем – ASCII-символы. Данный метод не нашел широкого применения ввиду его высокой стоимости и наукоемкости.

Верификация полученных результатов. К сожалению, довольно часто программные продукты, предназначенные для криминалистического исследования мобильных устройств, извлекают данные не полностью. Поэтому верификация полученных в ходе исследования цифровых улик является неотъемлемой частью производства судебной экспертизы.

Существует несколько способов верификации полученных результатов. К наиболее распространенным относятся следующие:

– сравнение полученных в ходе исследования данных с данными, отображающимися мобильным устройством;

– сравнение полученных данных с данными в шестнадцатеричном представлении, имеющимися в побитовой копии внутренней памяти мобильного устройства;

– использование нескольких программных продуктов при извлечении данных из мобильного устройства и последующее сравнение полученных результатов.

Составление Заключения

Заключение должно содержать: дату и время начала и окончания исследования; сведения о физическом состоянии мобильного устройства, фотографии его внешнего вида, наклейки с идентифицирующей его информацией, а также SIM-карты и карты памяти (если имеются); сведения о состоянии телефона, в котором он поступил на экспертизу (включен/выключен); сведения о производителе, модели и других идентификационных данных устройства; сведения об используемом при производстве экспертизы программном обеспечении; сведения о методиках, используемых при производстве экспертизы; сведения о категориях данных, обнаруженных в ходе исследования и их содержании.

Выводы, к которым эксперт пришел по итогам производства судебной экспертизы, должны быть краткими и однозначными, соответствовать поставленным на разрешение эксперта вопросам.

ВЫВОДЫ

С учетом анализа указанных в исследовании данных и практики мы пришли к выводу о том, что на данный момент в мире не существует универсального программного обеспечения для проведения исследования мобильных устройств. Применение одного или двух программных обеспечений или аппаратно-программных комплексов не достаточно так как каждая модель и марка

производителя требует отдельного подхода, причиной тому является то что из года в год с выпуском новых моделей мобильных телефонов производители усиливают уровень защиты мобильных устройств с целью защиты информации своих потребителей, в связи с чем необходимо постоянно ввести разработку новых видов экспертного исследования мобильных устройств, ввести тесное сотрудничество со странами имеющими богатый опыт расследовании инцидентов связанных с исследованием мобильных устройств, участвовать проектах по обмену опытом и проводить совместные исследования.

Библиографические ссылки

1. Постановление Президента Республики Узбекистан №-4024 от 21 ноября 2018 г. «О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты» [Электронный ресурс]. – Режим доступа: https://lex.uz/docs/4071399 - (Дата обращения: 27.11.2020).

2. Крестовников О.А. Информационные технологии в борьбе с преступностью. – 2013. – № 6. – С. 278-282.

3. Игорь Михайлов. Основы криминалистического исследования мобильных устройств. – Федотов, Н.Н. Форензика – компьютерная криминалистика / Н.Н. Федотов. – М.: Юридический мир, 2007. – 360 с. [Электронный ресурс]. – Режим доступа: https://www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-issledovaniya-mobilnykh-ustrojstv – Дата обращения: 27.11.2020.;

4. Игорь Михайлов. Основы криминалистического исследования мобильных устройств – Casey, E. DigitalEvidenceandComputerCrime, ThirdEdition: Forensic Science, Computers, andtheInternet / E. Casey. – NYC: AcademicPress, 2011. – 840 p. [Электронный ресурс]. – Режим доступа: https ://www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-ssledovaniya-mobilnykh-ustrojstv – (Дата обращения: 27.11.2020)/

5. Государственный визит Президента Республики Корея Мун Чжэ Ин 18 апреля в Узбекистан. – Режим доступа: https://uz.sputniknews.ru/politics/20190418/11282818/Tsvety-i-pochesti-kak-yuzhnokoreyskogo-lidera-vstrechali-v-Tashkente. – Дата обращения: 27.11.2020 г.

6. Аппаратно-программный комплекс для съема и исследования данных из мобильных устройствUFED 4PC– Режим доступа: http://aimtech.ru/catalog/154. – Дата обращения: 27.11.2020.

7. **Государственный стандарт Республики Узбекистан**. Методы обеспечения безопасности. Руководящие указания по идентификации, сбору, получению и сохранению цифровых доказательств (ISO/IEC 27037:2012, MOD) – С. 7-8.

8. Игорь Михайлов. Основы криминалистического исследования мобильных устройств – [Электронный ресурс]. – Режим доступа: https ://www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-ssledovaniya-mobilnykh-ustrojstv – (Дата обращения: 27.11.2020);

9. Игорь Михайлов. Основы криминалистического исследования мобильных устройств – Developing Process for Mobile Device Forensics [Электронный ресурс]. – Режим доступа: https ://www.oxygensoftware.ru/ru/news/articles/83-osnovy-

kriminalisticheskogo-ssledovaniya-mobilnykh-ustrojstv – (Дата обращения: 27.11.2020);

10. Игорь Михайлов. Основы криминалистического исследования мобильных устройств – Brothers, S. iPhone Tool Classification [Электронный ресурс]. – Режим доступа: https ://www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-ssledovaniya-mobilnykh-ustrojstv – (Дата обращения: 27.11.2020)

REFERENCES:

1. Resolution of the President of the Republic of Uzbekistan No. -4024 of November 21, 2018 "on measures to improve the system of control over the introduction of information technologies and communications, organization of their protection" [Electronic resource]. - Access mode: https://lex.uz/docs/4071399 - (accessed: 27.11.2020).

2. Krestovnikov O. A. Information technologies in the fight against crime. - 2013. - No. 6. - Pp. 278-282.

3. Igor Mikhailov. Fundamentals of forensic research of mobile devices. - Fedotov, N. N. Forenzika-computer criminalistics / N. N. Fedotov. - M.: Legal world, 2007. - 360 p. [Electronic resource]. - Access mode: https://www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-issledovaniya-mobilnykh-ustrojstv -accessed: 27.11.2020.;

4. Igor Mikhailov. Fundamentals of forensic research of mobile devices-Casey, E. DigitalEvidenceandComputerCrime, ThirdEdition: Forensic Science, Computers, andtheInternet / E. Casey. – NYC: AcademicPress, 2011. – 840 p. [Electronic resource]. - Access mode: https: //www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-ssledovaniya-mobilnykh-ustrojstv – (accessed: 27.11.2020)/

5. State visit of the President of the Republic of Korea moon Jae-In to Uzbekistan on April 18. – Mode of access: https://uz.sputniknews.ru/politics/20190418/11282818/Tsvety-i-pochesti-kak-yuzhnokoreyskogo-lidera-vstrechali-v-Tashkente. – Date of access: 27.11.2020 G.

6. Hardware and software package for data collection and research from mobile devicesufed 4PC-access Mode: http://aimtech.ru/catalog/154. - accessed: 27.11.2020.

7. State standard of the Republic of Uzbekistan. Security method. Guidelines for the identification, collection, receipt and preservation of digital evidence (ISO/IEC 27037: 2012, MOD) - Pp. 7-8.

8. Igor Mikhailov. Fundamentals of forensic research of mobile devices- [Electronic resource]. - Access mode: https: //www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-ssledovaniya-mobilnykh-ustrojstv – (accessed: 27.11.2020);

9. Igor Mikhailov. Fundamentals of forensic research of mobile devices-Developing Process for Mobile Device Forensics [Electronic resource]. - Access mode: https: //www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-ssledovaniya-mobilnykh-ustrojstv – (accessed: 27.11.2020);

10. Igor Mikhailov. Fundamentals of forensic research of mobile devices-Brothers, S. iPhone Tool Classification [Electronic resource]. - Access mode: https:

//www.oxygensoftware.ru/ru/news/articles/83-osnovy-kriminalisticheskogo-ssledovaniya-mobilnykh-ustrojstv – (accessed: 27.11.2020).