



ЮРИСТ АХБОРОТНОМАСИ

ВЕСТНИК ЮРИСТА * LAWYER HERALD

ҲУҚУҚИЙ, ИЖТИМОИЙ, ИЛМИЙ-АМАЛИЙ ЖУРНАЛ



CYBERLENINKA



НАУЧНАЯ ЭЛЕКТРОННАЯ
БИБЛИОТЕКА
LIBRARY.RU



ISSN 2181-9416

Doi Journal 10.26739/2181-9416

ЮРИСТ АХБОРОТНОМАСИ

3 СОН, 1 ЖИЛД

ВЕСТНИК ЮРИСТА

НОМЕР 3, ВЫПУСК 1

LAWYER HERALD

VOLUME 3, ISSUE 1



TOSHKENT-2020

**КОНСТИТУЦИЯВИЙ ҲУҚУҚ. МАЪМУРИЙ ҲУҚУҚ. МОЛИЯ ВА
БОЖХОНА ҲУҚУҚИ**

1. МАХМУДОВ Фируз Бахтиёр ўғли ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ҚОНУНЧИЛИГИДА ДАВЛАТ ФУҚАРОЛИК ХИЗМАТЧИЛАРИ УЧУН ЎРНАТИЛГАН ТАҚИҚ ВА ЧЕКЛОВ МАСАЛАЛАРИ.....	8
2. НАРИМАНОВ Бекзод Абдувалиевич ЎЗБЕКИСТОНДА НОДАВЛАТ НОТИЖОРАТ ТАШКИЛОТЛАР ТАРИХИ ВА РИВОЖЛАНИШИНИНГ АСОСИЙ ТЕНДЕНЦИЯЛАРИ.....	18

**ФУҚАРОЛИК ҲУҚУҚИ. ТАДБИРКОРЛИК ҲУҚУҚИ. ОИЛА ҲУҚУҚИ.
ХАЛҚАРО ХУСУСИЙ ҲУҚУҚ**

3. ИСМАИЛОВ Баходир Исламович, Маманов Сардоржон Собир ўғли ФОРМИРОВАНИЕ СИСТЕМ КОМПЛЕКСНОГО КОНТРОЛЯ КАК ЭФФЕКТИВНОГО ИНСТРУМЕНТА ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ В ЧАСТНОМ СЕКТОРЕ.....	30
4. АБДУЛЛАЕВ Хуршидjon Назрулло ўғли АУДИТОРЛИК ФАОЛИЯТИНИНГ ТАШКИЛИЙ- ҲУҚУҚИЙ АСОСЛАРИ.....	37
5. JAMOLOV Azizjon TERM OF SUBJECTS OF INVESTMENT ACTIVITY: THEORETICAL AND COMPARATIVE LEGAL ANALYSIS.....	44
6. EGAMOVA Dilrabo Talibovna KREDIT TALABLARI BO'YICHA INTELLEKTUAL MULK OBYEKTLARIGA NISBATAN UNDIRUVNI QARATISH MASALALARI.....	49
7. АҲРОРҚУЛОВ Анвар НОДАВЛАТ НОТИЖОРАТ ТАШКИЛОТЛАРИНИНГ МУЛКИЙ АСОСЛАРИ.....	56
8. АЛМОСОВА Шаҳноза ТРИПС БИТИМИ НОРМАЛАРИНИ ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ИНТЕЛЛЕКТУАЛ МУЛК ҚОНУНЧИЛИГИГА ИМПЛЕМЕНТАЦИЯ ҚИЛИШ МУАММОЛАРИ.....	63

**ФУҚАРОЛИК ПРОЦЕССУАЛ ҲУҚУҚИ. ИҚТИСОДИЙ ПРОЦЕССУАЛ
ҲУҚУҚИ. ҲАКАМЛИК ЖАРАЁНИ ВА МЕДИАЦИЯ**

9. ОТАХОНОВ Фозилжон Хайдарович НИЗОЛАРНИ МУҚОБИЛ ҲАЛ ЭТИШНИНГ ТАШКИЛИЙ-ҲУҚУҚИЙ МЕХАНИЗМЛАРИ ТАКОМИЛЛАШМОҚДА.....	72
--	----

**ЖИНОЯТ ҲУҚУҚИ, ҲУҚУҚБУЗАРЛИКЛАРНИНГ ОЛДИНИ ОЛИШ.
КРИМИНОЛОГИЯ. ЖИНОЯТ-ИЖРОИЯ ҲУҚУҚИ**

10. КАРАКЕТОВА Дилноза Юлдашевна ОФИРЛАШТИРУВЧИ ҲОЛАТ СИФАТИДА ЁШ БОЛА, ҚАРИЯ, НОГИРОН ЁКИ ОЖИЗ АҲВОЛДАГИ ШАХСЛАРНИ ХЎРЛАБ СОДИР ЭТИЛГАН БЕЗОРИЛИК УЧУН ЖАВОБГАРЛИК.....	80
11. ХЎЖАҚУЛОВ Сиёвуш Бахтиёрвич	

МУНДАРИЖА/СОДЕРЖАНИЕ/CONTENT

ҲУҚУҚБУЗАРЛИКЛАР УМУМИЙ ПРОФИЛАКТИКАСИНИНГ ҲУҚУҚИЙ ТАВСИФИ.....	88
---	----

ЖИНОЯТ ПРОЦЕССИ. КРИМИНАЛИСТИКА, ТЕЗКОР-ҚИДИРУВ ҲУҚУҚ ВА СУД ЭКСПЕРТИЗАСИ

12.МАТЧАНОВ Алимжан Атабаевич УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИ.....	96
13.ЮГАЙ Людмила Юрьевна ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ СУДЕБНОЙ ЭКСПЕРТИЗЫ В РЕСПУБЛИКЕ УЗБЕКИСТАН.....	104
14.ЗУЛФУҚОРОВ Абдувахоб Абдумалик ўғли ЙЎЛ-ТРАНСПОРТ ҲОДИСАСИ БЎЙИЧА ТРАСОЛОГИК ЭКСПЕРТИЗАСИНИ РИВОЖЛАНТИРИШ МАСАЛАЛАРИ.....	112

ХАЛҚАРО ҲУҚУҚ ВА ИНСОН ҲУҚУҚЛАРИ

15.СУЛАЙМАНОВ Одилжон Раббимович ХАЛҚАРО ВА МИНТАҚАВИЙ ҲУЖЖАТЛАРДА ИШНИНГ МУСТАҚИЛ ВА ХОЛИС СУД ТОМОНИДАН КЎРИБ ЧИҚИЛИШИ ҲУҚУҚИ.....	118
16.ГАФФАРОВА Шахноза Нуритдиновна ЎЗБЕКИСТОНДА ХОТИН-ҚИЗЛАР ВА ЭРКАКЛАР ТЕНГ ҲУҚУҚЛИЛИГИНИ ТАЪМИНЛАШ.....	126

ҲУҚУҚИЙ АМАЛИЁТ ВА ХОРИЖИЙ ТАЖРИБА

17.АЛИМОВ Гайбулла Алимович ЮРИДИК ШАХСЛАР ЖАВОБГАРЛИГИ: АМЕРИКА ҚЎШМА ШТАТЛАРИ ТАЖРИБАСИ.....	134
18.ХАМДАМОВА Фируза Уразалиевна "ОДИН ПОЯС, ОДИН ПУТЬ" КАК СРЕДСТВО КУЛЬТУРНОЙ ИНТЕГРАЦИИ, ИНСТРУМЕНТ УКРЕПЛЕНИЯ МЕЖДУНАРОДНЫХ НАУЧНЫХ СВЯЗЕЙ ИИ КАТАЛИЗАТОР РАЗВИТИЯ НАУКИ В ЭПОХУ ЦИФРОВОЙ ЭКОНОМИКИ.....	141

ЮРИСТ АХБОРОТНОМАСИ ВЕСТНИК ЮРИСТА LAWYER HERALD

ЖИНОЯТ ПРОЦЕССИ. КРИМИНАЛИСТИКА, ТЕЗКОР-ҚИДИРУВ ҲУҚУҚ ВА СУД ЭКСПЕРТИЗАСИ

МАТЧАНОВ Алимжан Атабаевич

Исполняющий обязанности профессора
Академии МВД Республики Узбекистан,
доктор юридических наук, доцент
E-mail: alimjan-60@inbox.uz

ОТДЕЛЬНЫЕ ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

For citation (иктибос келтириш учун, для цитирования): МАТЧАНОВ А.А.
ОТДЕЛЬНЫЕ ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПРИ РАССЛЕДОВАНИИ
КИБЕРПРЕСТУПЛЕНИЙ // Юрист ахборотномаси - Вестник юриста - Lawyer
herald. № 3 (2020), С.96-103.



№3 (2020) DOI <http://dx.doi.org/10.26739/2181-9416-2020-3-12>

АННОТАЦИЯ

В статье анализируются проблемы, которые связаны с отдельными особенностями доказывания при расследовании киберпреступлений. Эти особенности отражают алгоритм действий направленный на обнаружение, сбор, проверку и оценку новых разновидностей доказательств, выраженных в цифровой (электронной) форме. Изучен зарубежный опыт и мнения ученых о понятии и сущности цифровых (электронных) доказательств, порядок проведения следственного действия (осмотра), направленного на их сбор, фиксацию и определение уголовно-процессуальных особенностей этого вида доказательств.

Ключевые слова: киберпреступление, доказывание, процесс обнаружения доказательств, цифровые доказательства, электронные доказательства, информационно-коммуникационные технологии, Интернет, уголовно-процессуальный порядок, алгоритм.

МАТЧАНОВ Алимжан Атабаевич

Ўзбекистон Республикаси ИИВ Академияси профессори вазифасини
бажарувчи, юридик фанлар доктори, доцент
E-mail: alimjan-60@inbox.uz

КИБЕРЖИНОЯТЛАРНИ ТЕРГОВ ҚИЛИШДА ИСБОТ ҚИЛИШНИНГ

АЛОҲИДА ХУСУСИЯТЛАРИ**АННОТАЦИЯ**

Мақолада кибержиноятларни тергов қилишда исбот қилишнинг алоҳида хусусиятлари билан боғлиқ муаммолар таҳлил қилинган. Рақамли (электрон) шаклдаги далилларни топиш, тўплаш, текшириш ва баҳолаш характлар алгоритми хусусиятларни ифодалайди. Рақамли (электрон) далилларни тушунчаси ва моҳияти, ушбу турдаги далилларни тўплаш, қайд этиш ва жиноят-процессуал хусусиятларни аниқлашга қаратилган (куздан кечириш) тергов харакатини ўтказиш тартибининг хорижий тажриба ва олимларнинг фикрлари ўрганилган

Калит сўзлар: кибержиноятлар, исбот қилиш, далиларни топиш жараёни, рақамли далиллар, электрон далиллар, ахборот-коммуникацион технологиялар, Интернет, жиноят-процессуал тартиби, алгоритм.

MATCHANOV Alimjan

Acting Professor of the Academy of the MIA of the Republic of Uzbekistan

Doctor of Law Sciences, Associate professor

E-mail: alimjan-60@inbox.uz

SEPARATE FEATURES TO PROVE AT INVESTIGATION OF CYBERCRIMES**ANNOTATION**

In article problems which are connected with separate features to prove at investigation of cybercrimes are analyzed. These features reflect algorithm of actions directed on detection, collecting, check and an estimation of a new version of the proofs expressed in the digital (electronic) form. Foreign experience and opinions of scientists on concept and essence of digital (electronic) proofs, an order of carrying out of the investigatory action (survey) directed on their gathering, fixing and definition of criminally-remedial features of the given kind of proofs is studied.

Keywords: Cybercrimes, to prove, process of detection of proofs, digital proofs, electronic proofs, information-communication technologies, the Internet, a criminally-remedial order, algorithm.

Среди транснациональных преступлений, таких как: терроризм, экстремизм, незаконный оборот наркотических и психотропных веществ, торговля людьми, коррупция особое место занимают преступления в сфере информационных, телекоммуникационных технологий, которые именуются как киберпреступления.

Эти преступления стали настоящей проблемой транснационального масштаба, и мировые аналитические агентства приводят данные о нанесении огромного материального вреда, наносимого общественно-опасными деяниями в сфере информационных технологий (киберпреступлений). К 2022 году, по прогнозу Всемирного экономического форума, сумма всемирного ущерба от кибератак вырастет до 8 триллионов долларов США. В исследовании Zurich Insurance Group ущерб от злоумышленников и затраты на обеспечение кибербезопасности в Интернете оцениваются в 120 триллионов долларов США к 2030 году [1].

Современные проблемы, связанные с возрастающим числом преступлений в сфере информационно-коммуникационных технологий (далее ИКТ) или киберпреступность, приобрели всемирный характер и не ограничиваются какой-либо страной или регионом, а представляют собой угрозу всему мировому

сообществу. Обстановка в мире демонстрирует необходимость совершенствования механизма сотрудничества в доказывании при расследовании киберпреступлений.

Следует признать, что киберпреступления отличаются от правонарушений в сфере информационных технологий. На наш взгляд, первое понятие шире, чем второе и более точно отражает природу такого явления, как преступность в информационно-телекоммуникационном пространстве. Термин "киберпреступления" можно воспринимать как общественно-опасные деяния, связанные с совершением преступлений, в сфере информационно-коммуникационных технологий, где сама электронная информация, техника или ресурсы, с помощью которой совершаются преступления, составляют признаки этих противоправных деяний.

Процесс развития и совершенствования ИКТ и распространения в глобальном, международном пространстве посредством информационной интеграции, создал благоприятные условия для совершения киберпреступлений. Это потребовало от правоохранительных органов государств создать и оптимизировать механизм получения нового вида цифровых (электронных) доказательств [2, Р.155].

Н.А. Нугманов среди проблем связанных с применением информационных технологий анализирует такую как создание правовых условий для электронного документа в качестве доказательства в уголовном процессе [3, С.42].

А.У. Расулев в своем исследовании отмечает, что повышению эффективности борьбы с преступлениями в сфере информационных технологий имеется и такое приоритетное направление как обеспечение принципа неотвратимости ответственности за киберпреступления в сфере экономики путем раскрытия их юридической природы [4, С.37].

Анализ уголовно-процессуального законодательства Узбекистана (ст. 81 УПК) показал, что доказательствами по уголовному делу являются любые фактические данные, на основе которых, в определенном законом порядке, орган дознания, следователь и суд устанавливают наличие или отсутствие общественно опасного деяния, виновность лица, совершившего это деяние, и иные обстоятельства, имеющие значения для правильного разрешения дела.

Эти данные устанавливаются: показаниями свидетеля, потерпевшего, подозреваемого, обвиняемого, подсудимого, заключением эксперта, вещественными доказательствами, материалами звукозаписи, видеозаписи и кинофотосъемки, протоколами следственных и судебных действий и иными документами (курсивом выделено нами М.А.). Доказательства, полученные посредством информационных технологий, в силу особенностей их фиксирования, приобретают иные специфические формы, которые отличаются от предусмотренных в действующем УПК. Эти особенности создали предпосылки для возникновения в уголовном процессе таких специфических форм как цифровые или электронные доказательства.

Относительно этого Е.С. Ермакова отмечает, что "электронные доказательства легко подвергаются изменениям и мгновенному уничтожению. В силу этого, особую важность приобретает их своевременная и правильная фиксация. На наш взгляд, можно выделить следующие особенности фиксации электронных доказательств: 1) Оперативность; 2) Участие специалиста; 3) Наличие специальных устройств для их записи, сохранения и воспроизведения" [5, С.86]. На наш взгляд эти особенности при расследовании киберпреступлений наиболее полно отражают уголовно-процессуальный алгоритм, который необходимо знать сотрудникам правоохранительных органов.

Анализ зарубежного опыта показал, что в некоторых странах и, в частности,

в уголовно-процессуальном кодексе Вьетнама еще в 2015 году были внесены изменения, согласно которым, в качестве самостоятельного вида доказательств были определены "электронные данные". При этом были закреплены и присущие только этому источнику доказательств характеристики, а именно факт формирования цифровых сигналов в виртуальном пространстве.

Опыт расследования киберпреступлений в другой стране - США предусматривает использование цифровых доказательств как одного из основных средств установления обстоятельств дела. Для получения подобных доказательств были созданы специальные технические группы по исследованию цифровых доказательств - Technical Working Group on Digital Evidence (TWGDE), впоследствии были преобразованы в единую Scientific Working Group on Digital Evidence (SWGDE) (Официальный сайт - <http://ncfs.org/swgde/>).

По нашему мнению вышеуказанный зарубежный опыт показывает значение инновационных достижений информационных, коммуникационных технологий, которые могут быть использованы для получения цифровых (электронных) доказательств. Этот вид доказательств в настоящее время стал приобретать самостоятельное значение, как необходимая часть расследования киберпреступлений.

В Узбекистане также осуществляется правотворческая работа по урегулированию проблем связанных с использованием инновационных технологий по фиксации цифровых доказательств в уголовном процессе. В частности Законом Республики Узбекистан от 23 мая 2019 года № ЗРУ-542 (Национальная база данных законодательства, 24.05.2019 г., № 03/19/542/317) УПК был дополнен статьями 911 - 914, которые регулируют производство, основания, условия, порядок, закрепление хода и результатов следственного действия, проведенного в режиме видеоконференцсвязи. Для того, чтобы эти средства доказывания имели правовое основание необходимо закрепить за цифровыми доказательствами их правовой статус как отдельный, самостоятельный вид.

Н.А. Иванов дал собственное авторское определение цифровым доказательствам, которое наиболее полно отражает их уголовно-процессуальные особенности. По его мнению, под цифровыми доказательствами понимаются фактические сведения, полученные с помощью информационно-коммуникационных технологий дискретных сигналов, содержащихся или зафиксированных на компьютерных или иных машинных носителях, изъятую, переданную участниками процесса или полученную иным способом в соответствии с действующим уголовно-процессуальным законодательством [6, С.78].

Одним из основных средств обнаружения и фиксирования цифровых доказательств является изъятие электронных носителей при проведении следственного осмотра, как следственного действия.

В.А. Мещеряков, В.В. Трухачев относительно осмотра, как средства обнаружения и изъятия цифровых (электронных) доказательств, установили особую важность данного следственного действия отметив, что "арсенал имеющихся процессуальных действий достаточно велик, он все же, с одной стороны, ограничен, исчерпывающим списком, а с другой - в рассматриваемых нами целях фактически сводится к одному единственному следственному действию - осмотру" [7, С.108]. Это связано с тем, что осмотр является универсальным следственным действием, в котором восприятие цифровой информации предусматривает наличие определенных технических средств и необходимого программного обеспечения, позволяющего понять сущность информации, выраженной в цифровой форме.

Органы, ответственные за расследование преступлений, не всегда имеют дело

непосредственно с физическим электронным носителем информации. Особенность информационных, телекоммуникационных систем выражается в том, чтобы получить соответствующие цифровые доказательства, имеющие значение для расследования уголовного дела, не имея физического доступа к месту нахождения информационного носителя. При этом цифровая информация фиксируется в составляемом протоколе осмотра с использованием доступных для пользователей открытых источников, но только в том случае, когда данные размещены на общедоступных машинных, компьютерных или иных информационных носителях [8, С.171].

В отличие от осмотра, обыск и выемка являются средством, направленным на возможность активного поиска и принудительного изъятия необходимой доказательственной цифровой информации. Эти следственные действия проводятся с физическим проникновением в помещение, где находятся их машинные, электронные и иные информационные носители, с последующим изъятием либо самих физических носителей, либо копирования (переноса) информации на другие носители.

Таким образом, перед органами предварительного следствия, при расследовании киберпреступлений, возникает проблема фиксирования цифровых доказательств, полученных с информационных носителей и имеющих форму цифровых (электронных) доказательств. При этом, вышеуказанный вид доказательств может быть зафиксирован на любом материальном носителе, в том числе, полученном в результате применения и использования информационно-телекоммуникационных технологий. В сущности, они материализуются как вещественные доказательства или электронный документ посредством ИКТ, как сведения, представленные в форме цифровых сигналов материальным, машинным (электронным) носителем, независимо от средств их хранения, обработки и передачи. Это могут быть аппаратные и программные средства микропроцессорной техники. При этом доказательственную базу составляет информация, зафиксированная на машинных носителях или на CD-дисках, DVD-дисках, флешнакопителях (переносимые носители), а также встроенных в средства микропроцессорной, компьютерной или иной инновационной техники.

Н.А. Иванов считает сами машинные носители информации как источник доказательств. Он предлагает рассматривать их с двух точек зрения: как искусственно созданный материальный объект, предназначенный для хранения информации в дискретной форме и как информацию, записанную на машинном (электронном) носителе, вне зависимости от типа последнего [9, С. 75].

В сущности, цифровые доказательства при расследовании киберпреступлений представляют собой фактические сведения, хранящиеся в материальном носителе, основу работы которого составляют информационные или иные телекоммуникационные технологии, представленные в электронном или ином инновационном виде.

В. Б. Вехов, исследуя проблему работы с цифровыми (электронными) доказательствами, отмечает, что информация, хранящаяся на цифровых носителях, допускается в качестве доказательств в уголовном деле, если эта информация использовалась в качестве средства совершения преступления; сохранила на себе следы преступления; является предметом преступления; служит средством для обнаружения преступления и установления обстоятельств уголовного дела; содержит сведения, имеющие значение для установления обстоятельств, подлежащих доказыванию по уголовному делу [10, С.23]. По мере развития инновационных цифровых технологий, достижений науки и техники, а также

теории доказательств, расширяются возможности применения научно-технических средств направленных на обнаружение, фиксацию, изъятие, сохранение вещественных объектов в качестве цифровых (электронных) доказательств.

При получении, проверке и приобщении цифровых (электронных) доказательств по расследуемому уголовному делу по киберпреступлениям все процедуры осуществляется на основании действующего уголовно-процессуального законодательства с привлечением специалистов имеющих соответствующую квалификацию в сфере информационных и иных инновационных, цифровых технологий.

С практической точки зрения в расследовании киберпреступлений наибольшего внимания заслуживает деление объектов электронных доказательств по характеру связи с расследуемым событием и источнику сведений об обстоятельствах, подлежащих доказыванию.

В.Б. Вехов, Б.П. Смагоринский и С.А. Ковалев предлагают свою классификацию цифровых (электронных) доказательств. По их мнению, к ним следует отнести: файл, сетевой адрес, доменное имя, электронное сообщение, электронный документ, информационная система, сайт в сети Интернет, электронная подпись, компьютерная программа, база данных. электронный журнал, электронные денежные средства [11, С.14].

Н.А. Иванов, в свою очередь, указывает на несколько иную, более обобщенную классификацию цифровых (электронных) доказательств. По его мнению, в первую, самую большую группу входят доказательства, созданные с помощью текстовых редакторов (например, Word Pad) и текстовых процессоров (MS Word), файлы электронных таблиц, созданные с помощью MS Excel или аналогичных программ, а также файлы баз данных, создаваемых, например, с помощью MS Access. В эту же группу он относит и файлы электронных сообщений, передаваемых посредством e-mail, SMS-MMS сообщения. Вторая группа электронных доказательств состоит из файлов графических форматов, создаваемые с помощью программ растровой и векторной графики, а также графические файлы, создаваемые с помощью сканеров и цифровых фотоаппаратов (в т.ч. встроенных в средства мобильной связи). И наконец, третью группу составляют аудиовизуальные файлы, куда относятся звуковые файлы, а также файлы, содержащие динамические изображения (фильмы) [12, С. 77].

Изучение свойств и признаков информационных объектов при расследовании киберпреступлений во многих случаях позволяет дать правильную правовую оценку. Характеризуя значение цифровых (электронных) доказательств, в качестве нового вида, следует обратить на их индивидуальность, отраженную в цифровых или иных информационных, телекоммуникационных носителях. Возможность же восполнения сведений, содержащихся в утраченных или отсутствующих источниках, за счет других зависит не от механизма их формирования, а от конкретных обстоятельств дела.

В настоящее время возникла объективная необходимость учитывать уголовно-процессуальные особенности доказывания при расследовании киберпреступлений. По нашему мнению, уголовно-процессуальный порядок доказывания при совершении киберпреступлений, посредством использования цифровых (электронных) доказательств, имеет своеобразный алгоритм и его необходимо закрепить как отдельный вид доказательства. Эти доказательства, отраженные в цифровом формате, содержатся в информационном машинном или ином инновационном носителе при расследовании киберпреступлений.

Исходя из вышеизложенного считаем целесообразным в ч. 2 ст. 81 УПК внести

соответствующие изменения изложив в следующей редакции: "Эти данные устанавливаются: показаниями свидетеля, потерпевшего, подозреваемого, обвиняемого, подсудимого, заключением эксперта, вещественными доказательствами, материалами звукозаписи, видеозаписи, кинофотосъемки, информационно-телекоммуникационными носителями, цифровыми доказательствами, протоколами следственных и судебных действий и иными документами".

Таким образом, можно сделать вывод, что обнаружение и фиксация цифровых (электронных) доказательств при расследовании киберпреступлений представляет собой сложный процесс, сочетающий в себе комплекс мероприятий, связанных с уголовно-процессуальным порядком, криминалистической методикой и тактикой обнаружения, получения и оценки этих доказательств. Знание и умение на практике применить весь арсенал международного опыта работы с цифровыми (электронными) доказательствами позволит создать оптимальный механизм уголовно-процессуального порядка и алгоритма расследования киберпреступлений.

Иқтибослар/Сноски/References

1. <https://www.kommersant.ru/doc/3957187>.
2. Tropina, T., Self- and Co-regulation in Fighting Cybercrime and Safeguarding Cybersecurity. In: Jhnke at al. (eds.), "Current Issues in ITU Security", Duncker & Humblot, Berlin, 2012. P. 155.
3. Нугманов Н. А. Теоретико-практические особенности формирования международного информационного права: Автореф. дис. ...док. юрид. наук (DSc). - Т., 2018. - 59 с. (Nugmanov H. A. Teoretiko-practical features of formation of the international information right: : Abstract. dis. ... Dr. jur. Science (DSc).- T, 2018. - 59 p.)
4. Расулев А.У. Совершенствование уголовно-правовых и криминалистических мер борьбы с преступлениями в сфере информационных технологий и безопасности: Автореф. дис. ...д-ра юрид. Наук (DSc). - Т., 2018. - 74 с. (Rasulev A.U. Perfection criminally-legal and криминалистических measures of struggle against crimes in sphere of information technology and safety: : Abstract. dis. ... Dr. jur. Science (DSc).- T, 2018. - 74 p)
5. Ермакова Е. С. Электронные доказательства как новое направление в практике расследования преступлений / Е. С. Ермакова, Д. М. Джумангалиева. - Текст : непосредственный // Молодой ученый. - 2018. - № 23 (209). - С. 85-87. - URL: <https://moluch.ru/archive/209/51196/> (дата обращения: 05.06.2020). (Ermakova E. S. Electronic proofs as a new direction in practice of investigation of crimes / E.S.Ermakova, D. M.Dzhumangalieva. - the Text: direct//the Young scientist. - 2018. - № 23 (209). - P. 85-87. - URL: <https://moluch.ru/archive/209/51196/>(reference date: 6/5/2020).
6. Иванов Н.А. О понятии "цифровые доказательства" // Вестник Омского юридического института, 2006, № 2 (5), - С. 77-78. (Ivanov N.A. About concept "digital proofs"/the Bulletin Omsk legal Institute, 2006, № 2 (5) - P. 77-78)
7. Мещеряков В.А., Трухачев В.В. Формирование доказательств на основе электронной цифровой информации // Вестник Воронежского института МВД России. 2012. №2. - С.108-110. (Meshcherjakov V. A, Truhachev V.V. Formirovanie of proofs on the basis of the electronic digital information//the Bulletin of the Voronezh institute of the Ministry of Internal Affairs of Russia. 2012. №2. - P.108-110)
8. Карташов И.И. Нетрадиционные источники оперативной информации // Актуальные проблемы деятельности подразделений УИС: сборник материалов открытой научно-практической конференции / ФГОУ ВПО Воронежский институт ФСИН России. - Воронеж: Научная книга, 2010. - С. 169 - 174. С. 171. (Kartashov

I.I. Nonconventional sources of the operative information//Actual problems of activity of divisions UIS: the collection of materials of open scientifically-practical conference / FGOU ВПО the Voronezh institute FSIN of Russia. - Voronezh: the Scientific book, 2010. - С. 169 - 174. P. 171)

9.Иванов Н.А. Транснациональные преступления, совершаемые с использованием компьютерных и телекоммуникационных технологий (классификация, теория и практика расследования): Специализированный учебный курс / Под. ред. д.ю.н. Н.А. Лопашенко. Саратов: Саратовский Центр по исследованию проблем организованной преступности и коррупции, 2007. - 75-77. (Ivanov N.A. Transnational the crimes made with use of computer and telecommunication technologies (классификация, the theory and investigation practice): the Specialized training course / Under. ред. д.ю.н. N.A.Lopashenko. Saratov: the Saratov Center on research of problems of the organised crime and corruption, 2007. - P.75-77.)

10.Вехов В. Б. Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. - 2013. - № 10. - С. 22-24. (Vehov V.B.Work with electronic evidence in the context of the changed criminal procedure legislation //the Russian inspector. - 2013. - № 10. - P. 22-24)

11.Вехов В. Б., Смагоринский Б. П., Ковалев С. А. Электронные следы в системе криминалистики // Судебная экспертиза. - 2016. - № 2 (46). - С. 10-19. (Vehov V. B. of Century B., Smagorinsky B. П, Kovalev With. And. Electronic traces in criminalistics system//Judicial examination. - 2016. - № 2 (46). -P. 10-19)

12.Иванов Н.А. Транснациональные преступления, совершаемые с использованием компьютерных и телекоммуникационных технологий (классификация, теория и практика расследования): Специализированный учебный курс / Под. ред. д.ю.н. Н.А. Лопашенко. Саратов: Саратовский Центр по исследованию проблем организованной преступности и коррупции, 2007. - 115 с. (Ivanov N.A. Transnational the crimes made with use of computer and telecommunication technologies (классификация, the theory and investigation practice): the Specialized training course / Under. N.A.Lopashenko. Saratov: the Saratov Center on research of problems of the organised crime and corruption, 2007. - 115 p)