

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ  
РЕСПУБЛИКИ КАЗАХСТАН

АЛМАТИНСКАЯ АКАДЕМИЯ  
имени МАКАНА ЕСБУЛАТОВА



**АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ  
УГОЛОВНЫМ ПРАВОНАРУШЕНИЯМ  
В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ**

Материалы  
международной научно-практической конференции  
(22 мая 2020 г.)

Алматы  
2020

УДК 347.9(063)  
ББК 67.7  
Д 70 43

***Ответственный редактор:***

Смаилов О.Х. – начальник Алматинской академии  
МВД Республики Казахстан имени Макана Есбулатова,  
кандидат юридических наук, полковник полиции

***Редакционная коллегия:***

Дильбарханова Ж.Р., Бимолданов Е.М., Канапиев М.А.,  
Кан А.Г., Цой О.Р., Байсеитов Б.Т., Мурашбеков О.Б.

Д 70 Актуальные проблемы противодействия уголовным правона-  
рушениям в сфере информатизации и связи: мат-лы межд. науч.-прак.  
конф. – Алматы: ООНИиРИР Алматинской академии МВД Республики  
Казахстан им. М. Есбулатова, 2020. – 258 с.

ISBN 978-601-7963-60-6

В сборнике представлены научные доклады участников международной  
научно-практической конференции «Актуальные проблемы противодействия  
уголовным правонарушениям в сфере информатизации и связи».

Сборник конференции рассчитан на преподавателей, докторантов и маги-  
странтов высших учебных заведений правоохранительных органов, других юри-  
дических вузов, практических работников органов внутренних дел, а также ши-  
рокий круг читателей.

*Материалы, публикуемые в сборнике, даны в авторской редакции.*

ISBN 978-601-7963-60-6

УДК 340.9(063)  
ББК 67.7

© Алматинская академия МВД  
Республики Казахстан имени  
Макана Есбулатова, 2020

**МУСАБЕКОВ Е.А.,**

магистрант профильной магистратуры Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, квалификационный класс 3 категории службы экономических расследований

**ЕШНАЗАРОВ А.А.,**

доцент кафедры специальных юридических дисциплин Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, к.ю.н., советник юстиции

**ОСМОТР И НЕКОТОРЫЕ ПРОБЛЕМЫ  
РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ**

Осмотр один из основных следственных действий проводимый органами уголовного преследования от качества, которого зависит быстрое и полное раскрытие уголовных правонарушений. Эффективность расследования киберпреступлений также зависит от осмотра.

На сегодняшний день имеется достаточно отечественных и зарубежных работ, посвященных различным аспектам борьбы с киберпреступлениями [1, 2, 3, 4, 5, 6, 7, 8, 9 и др.].

Мы же рассмотрим отдельные уголовно-процессуальные проблемы осмотра.

***Дистанционный осмотр***

По мнению В.П. Хомколова при совершении одного киберпреступления, могут быть несколько мест происшествия:

– рабочее место, рабочая станция — место обработки информации, ставшей предметом преступного посягательства;

– место постоянного хранения или резервирования информации – сервер или стример;

– место использования технических средств для неправомерного доступа к компьютерной информации, находящейся в другом месте, при этом место использования может совпадать с рабочим местом, но находиться вне организации, например, при стороннем взломе путем внешнего удаленного сетевого доступа;

– место подготовки преступления (разработки вирусов, программ взлома, подбора паролей) или место непосредственного использования информации (копирование, распространение, искажение), полученной в результате неправомерного доступа к данным, содержащимся на ПК.

Местом происшествия может быть одно помещение, где установлен компьютер и хранится информация, ряд помещений, в том числе в разных зданиях, расположенных на различных территориях, либо участок местности, с которого проводится дистанционный электромагнитный или аудио перехват.

Также современные ученые выделяют новое для современной практики место совершения преступления, а именно информационное пространство (киберпространство), где не действуют географические, юридические законы и понятия. Существует ряд вопросов, как проводить специфический осмотр места происшествия, как фиксировать найденную информацию и придавать ей доказательственное значение [10, с.72].

Соглашаясь с изложенным, мы предлагаем классификацию исходя из действующего законодательства Казахстана. Осмотр по киберпреступлениям мы **классифицируем** на осмотр:

1) помещений:

- по месту проживания потерпевшего (физическое лицо).

В ходе осмотра также могут быть осмотрены компьютеры, смартфоны и иные электронные носители информации;

- по месту происшествия инцидента информационной безопасности (юридическое лицо);

В ходе осмотра организации могут быть осмотрены объекты информационно-коммуникационной инфраструктуры (информационные системы, технологические платформы, аппаратно-программные комплексы, серверные помещения (центры обработки данных), сети телекоммуникаций, а также системы обеспечения информационной безопасности и бес-

перебойного функционирования технических средств) п.25 ст. 1 ЗРК «Об информатизации»;

- по месту проживания (задержания) подозреваемого. В ходе осмотра также могут быть осмотрены компьютеры, смартфоны и иные электронные носители информации;

2) предмета (электронных носителей информации): компьютер, смартфон и иные электронные носители информации, изъятые с места происшествия, при обыске и выемке (дополнительный осмотр). А также при получении результатов негласного снятия информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации (ч. 3 ст. 245 УПК РК).

При систематизации видов осмотра как указали выше, мы ориентировались на ст. 219 УПК РК.

Полагаем, данная классификация должна быть дополнена третьим видом осмотра как **«дистанционный осмотр»**.

Дистанционный осмотр предлагается нами по следующим причинам.

По мнению О.Ю. Введенской основным элементом следовой картины интернет-преступлений будут являться информационные следы. Среди таких следов для всех рассмотренных преступных деяний могут быть характерны чаты, блоги, переписка, фотографии, skrinshots страниц, содержимое аккаунтов пользователей различных сайтов, сервисов, и т.п. [11, с.215].

А.Н. Колычева в качестве основных объектов фиксации доказательственной информации, размещенных в интернет-пространстве, относит сведения, указанные в ст. 74 УПК РФ: лог-файлы (протоколы автоматической регистрации события, происходящих при работе программного обеспечения), сведения о сетевых ресурсах, доменах, их владельцах, базы данных с информацией конфиденциальной характера [12, с.110].

Кроме того, дополнительными критерием выделения дистанционного осмотра являются:

1) в УПК РК уже имеется «дистанционный допрос» ст. 213 УПК РК;

2) в УК РК имеется Глава 7, посвященная уголовным правонарушениям в сфере информатизации и связи;

3) в Республике Казахстан принят Закон Республики Казахстан от 7 января 2003 года N 370 «Об электронном документе и электронной цифровой подписи».

Все это требует глубочайшей проработки вопросов в части:

- определения места электронных доказательств в теории доказательств;

- разграничения осмотра от обыска при получении компьютерной информации;

- криминалистического обеспечения следственных действий.

Учитывая рамки статьи, мы только обозначили данные проблемы, но каждая из этих проблем требуют отдельного диссертационного исследования.

В этой связи предлагаем, дополнить ст.219 УПК РК понятием дистанционный осмотр.

Осмотр электронных средств и электронных носителей

Между уголовным и уголовно-процессуальными кодексами имеются противоречия в понятийном аппарате.

В п. 41 ст. 3 УК РК раскрывается значение электронного носителя – это материальный носитель, предназначенный для хранения информации в электронной форме, а также записи или ее воспроизведения с помощью технических средств.

Сразу отметим, что данное определение полностью соответствует понятию «электронный носитель» содержащийся в Законе РК «Об информатизации» (п.60 ст. 1) [13].

Однако в ст. ст. 242 (*Негласные аудио- и (или) видеоконтроль лица или места*), 243 (*Негласные контроль, перехват и снятие информации, передающейся по сетям электрической (телекоммуникационной) связи*), 244 (*Негласное получение информации о соединениях между абонентами и*

*(или) абонентскими устройствами), 245 (Негласное снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации) УПК РК применяется понятие «материальный носитель».*

Учитывая, что УК РК и профильный закон применяет термин «электронный носитель» мы полагаем, что соответствующие поправки требуются внести в указанные статьи УПК РК в части приведения законодательства в единство применяемых понятий.

И к электронным носителям мы отнесем USB-флеш-накопители (флешки), жесткие диски и др. гаджеты, что может быть использовано для хранения информации в электронной форме.

Касательно компьютеров, ноутбуков, планшетов, смартфонов, гаджетов, видеотехники, аудиотехники, смарт-часов, электронных книг и многих других средств мы полагаем, необходимо обозначить как «электронные средства».

Во-первых, для их обобщения, во-вторых, чтобы не произошло смешивание понятий с научно-техническими средствами, которые используются в процессе доказывания и отличать их от электронных носителей, в-третьих, для использования электронной информации хранящихся в электронных средствах в качестве электронных доказательств.

Здесь мы согласны с мнением И.И. Литвина, который отметил, что целесообразно ввести новую категорию технических средств – «электронные средства».

Критерием, отличающим электронные средства от иных технических средств, является результат их применения – электронная информация, выраженная в виде электронного файла. Необходимость выделения отдельной категории вызвана потребностью внесения изменений в правовое регулирование применения данных средств, а также особый порядок использования электронной информации в качестве доказательств [14, с. 9].

Мы также поддерживаем И.И. Литвина о внесении в понятийный аппарат УПК РФ авторского понятия «электронные средства», где под электронными средствами понимаются любые технические средства, результатом применения которых является информация в электронном виде [14, с. 10].

Аналогичную дефиницию «электронные средства» необходимо закрепить в УПК РК.

Здесь мы отметим, что киберпреступления не имеют границ, и внесение схожих понятий в уголовно-процессуальное законодательство будет способствовать его унификации в рамках ЕАЭС и положительно отразится на эффективности расследования данного вида преступлений.

Таким образом, предлагаем свою классификацию осмотров по киберпреступлениям:

- осмотр помещений;
- дистанционный осмотр (осмотр, проводимый в интернет пространстве);
- осмотр электронных средств (технические средства, имеющие функцию записи, воспроизведения и хранения электронной информации);
- осмотр электронных носителей (технические средства, имеющие функцию хранения электронной информации).

Необходимо пояснить, что под осмотр предметов «электронные средства» и «электронные носители» подпадать не будут в связи с тем, что мы их выделяем в отдельный вид осмотра.

На основании изложенного предлагается внести соответствующие поправки в УПК РК:

1) ст. 7 УПК РК дополнить понятиями «электронные средства» и «электронные носители».

2) ст. 219 УПК РК дополнить видами осмотра как дистанционный осмотр, осмотр электронных средств, осмотр электронных носителей;

3) ст. ст. 221, 252, 253, 257, 259 УПК РК дополнить словами «электронных средств» и «электронных носителей»;

4) ст. ст. 242, 243, 244, 245 УПК РК слова «материальный носитель» заменить на слова «электронный носитель».

Полагаем, указанные предложения будут способствовать процессуальному закреплению доказательств, и исключат противоречия в практической деятельности правоохранительных органов, а также судов при оценке доказательств.

### **Литература**

1. Толеубекова Б.Х. Компьютерная преступность: уголовно-правовые и процессуальные аспекты: Учебное пособие. – Караганда: ВШ МВД СССР, 1991 г. - 82 с.

2. Толеубекова Б.Х. Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники // Дисс... на соискание ученой степени д.ю.н. - 1998 г. – 410 с.

3. Зинкевич Е.И. Основы криминалистической диагностики и идентификации компьютерных принтеров и документов, исполненных на них // Дисс... на соискание ученой степени к.ю.н. – 2000 г. – 184 с.

4. Сырбу А.В. Процессуальный порядок получения и использования информации с технических каналов связи в уголовном судопроизводстве // Дисс... на соискание ученой степени к.ю.н. – 2005 г. – 191 с.

5. Имангалиев Н.К., Темиржанова Л.А., Ешназаров А.А., Ажибаев М.Г., Дюсетаев Р.С. Алгоритм расследования киберпреступлений (особенности составления процессуальных документов): Практическое пособие / Под ред. А.В. Сырбу. – Астана: Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан. – 2018. – 174 с.

6. Ешназаров А.А., Имангалиев Н.К. Отдельные меры по противодействию преступлениям в сфере информационных технологий в Республике Казахстан // Хабаршы. Серия «Юриспруденция». – 2019. - № 2 (56). С.47-60.

7. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации судопроизводстве // Дисс... на соискание ученой степени д.ю.н. – 2001 г. – 385 с.

8. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений // Дисс... на соискание ученой степени к.ю.н. – 2016 г. – 249 с.

9. Крыгин С.В. Расследование преступлений, совершаемых в сфере компьютерной информации // Дисс... на соискание ученой степени к.ю.н. – 2002 г. – 200 с.

## Содержание

РОССИНСКАЯ Е.Р. ВЕКТОР ИННОВАЦИОННОГО РАЗВИТИЯ КРИМИНАЛИСТИЧЕСКОЙ НАУКИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ.....	3
VIMOLDANOV Y.M. ON THE GROUNDS OF CRIMINAL LIABILITY FOR THE CREATION, USE OR DISTRIBUTION OF MALICIOUS COMPUTER PROGRAMS AND SOFTWARE PRODUCTS .....	13
КАНАПЯЕВ М.А. КОМПЬЮТЕРЛІК ҚЫЛМЫС ҚАЗІРГІ ЗАМАНҒЫ КРИМИНОЛОГИЯЛЫҚ МӘСЕЛЕ РЕТІНДЕ.....	17
GALYASHINA E.I. DETECTION OF CRIMINAL CONTENT IN SOCIAL MEDIA (A FORENSIC LINGUISTIC APPROACH) .....	24
УТЕПОВ А.У. О ПРОТИВОДЕЙСТВИИ ПРОНИКНОВЕНИЮ И РАСПРОСТРАНЕНИЮ РАДИКАЛИЗМА И ИДЕЙ РЕЛИГИОЗНОГО ЭКСТРЕМИЗМА В ИНТЕРНЕТ-ПРОСТРАНСТВЕ .....	31
АХМЕТОВ И.А. АҚПАРАТТЫҚ-ПСИХОЛОГИЯЛЫҚ ӘСЕР ҚАЗІРГІ АҚПАРАТТЫҚ ҚАРАМА-ҚАЙШЫЛЫҚТЫҢ ҚҰРАМДАС БӨЛІГІ .....	48
ФЕДОРЕНКО О.А. ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ИНТЕРНЕТ ВЕЩЕЙ В СФЕРЕ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПНОСТИ.....	53
ПОЛИТОВА А.С., БИЛЕНКО П.С. КИБЕРБУЛЛИНГ: СПОРНЫЕ ВОПРОСЫ КВАЛИФИКАЦИИ .....	57
СЕМБИЕВ С.Ж. КРИПТОВАЛЮТАЛАР: ЖАҒЫМДЫ ҚАСИЕТТЕРІ МЕН КЕМШІЛІКТЕРІ.....	64
КАНАПЯЕВ М.А., БАЙСЕИТОВ Б.Т. ОСОБЕННОСТИ ПОЛУЧЕНИЯ ОПЕРАТИВНО-ЗНАЧИМОЙ ИНФОРМАЦИИ О КРАЖАХ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ .....	70

СЕРОВ И.А. НЕКОТОРЫЕ ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И ПРЕДУПРЕЖДЕНИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ .....	76
ЗИНКЕВИЧ Е.И. ВИРТУАЛЬНАЯ ВАЛЮТА (КРИПТОВАЛЮТА) КАК ОДИН ИЗ ЭЛЕМЕНТОВ ФОРМИРУЮЩИХ КРИМИНАЛИСТИЧЕСКУЮ ХАРАКТЕРИСТИКУ ПРЕСТУПЛЕНИЙ .....	83
ДЁМИН К.Е. О ДИДАКТИКЕ И СТАНДАРТИЗАЦИИ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ В РОССИЙСКОЙ ФЕДЕРАЦИИ .....	93
ЖҮНИСОВА Г.Ә. ЖАСӨСПІРІМДЕР АРАСЫНДА НАШАҚОРЛЫҚТЫҢ ТАРАЛУЫНА ҚАРСЫ ІС-ҚИМЫЛДАР .....	98
НИКИШИН В.Д. ДЕВИАНТНОЕ РЕЧЕВОЕ ПОВЕДЕНИЕ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕРНЕТ-КОММУНИКАЦИИ .....	104
КОРЖУМБАЕВА Т.М. ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ КРИПТОВАЛЮТ В РЕСПУБЛИКЕ КАЗАХСТАН .....	112
ГРАНКИНА В. ПРОБАЦИОННАЯ ДЕЯТЕЛЬНОСТЬ РЕСПУБЛИКИ КАЗАХСТАН И УКРАИНЫ КАК СПОСОБ ПРЕДУПРЕЖДЕНИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ .....	121
SHKOLNIKOV V. THE EXPERIENCE OF UKRAINE IN IMPLEMENTING THE CONVENTION ON CYBERCRIME.....	127
СЕМИКАЛЕНОВА А.И. ПРОБЛЕМЫ ИНФОРМАЦИОННО-КОМПЬЮТЕРНОГО ОБЕСПЕЧЕНИЯ СУДЕБНОЙ ЭКСПЕРТИЗЫ ЦИФРОВЫХ СЛЕДОВ.....	129
КРЫЖНАЯ В.В. ОСОБЕННОСТИ ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ.....	135

ТЫНДЫБАЕВ Қ.Қ., БАЙБОЛОВА А.А. «ҚАЗАҚСТАННЫҢ КИБЕРЩИТІ» ТҰЖЫРЫМДАМАСЫ ЖӘНЕ ОНЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ҮШІН МАҢЫЗЫ.....	139
КАБЫЛБЕКОВА А.С. ПРОФИЛАКТИКА КИБЕРЭКСТРЕМИЗМА СРЕДИ МОЛОДЕЖИ .....	146
СЕЙТАКОВА Б.М. ОСОБЕННОСТИ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ .....	154
ГРИГОРЬЕВ В.В. О СОСТОЯНИИ БОРЬБЫ С ТЕРРОРИЗМОМ И ЭКСТРЕМИЗМОМ В КАЗАХСТАНЕ.....	162
РАҚЫМ Е.Е., БЕКИШЕВ А.К. АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАРДЫҢ ЕРЕКШЕЛІКТЕРІ.....	174
НАСЫРОВА Э.М., САНАПИЯНОВА А.Н. КИБЕРҚЫЛМЫСТЫЛЫҚ: ДАМУ ТАРИХЫ, ТЕРГЕУ МЕН АШУ МӘСЕЛЕЛЕРІ .....	185
ДАУТОВА М.Ә. ИНТЕРНЕТ ЖЕЛІСІН ПАЙДАЛАНА ОТЫРЫП ЕСІРТКІ ҚҰРАЛДАРЫН САТУДЫ ТЕРГЕУ ЕРЕКШЕЛІКТЕРІ .....	191
АБЫЛКАСИМОВА А.Ш. ИНТЕРНЕТ ЖЕЛІСІ АРҚЫЛЫ КӨМЕЛЕТКЕ ТОЛМАҒАНДАР АРАСЫНДА СИНТЕТИКАЛЫҚ ЕСІРТКІНІҢ ТАРАЛУЫНЫҢ ӨЗЕКТІ МӘСЕЛЕЛЕРІ, ОЛАРДЫҢ САЛДАРЛАРЫ .....	198
АЛИМБЕКОВА Н. АҚПАРАТТАНДЫРУ ЖӘНЕ БАЙЛАНЫС САЛАСЫНДАҒЫ ТЕРІС ҚЫЛЫҚТАР ТУРАЛЫ ІСТЕР БОЙЫНША СОТҚА ДЕЙІНГІ ІС ЖҮРГІЗУ .....	206
МУСАБЕКОВ Е.А., ЕШНАЗАРОВ А.А. ОСМОТР И НЕКОТОРЫЕ ПРОБЛЕМЫ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ.....	213
ПРИХОДЬКО И.С. ИСПОЛЬЗОВАНИЕ СПЕЦИАЛЬНЫХ ЗНАНИЙ ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕПРАВОМЕРНЫМ ДОСТУПОМ	

К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.....	220
ШИДЕМОВ А.Г. КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМЫЕ АСПЕКТЫ УСТАНОВЛЕНИЯ ЛИЧНОСТИ - ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ .....	228
МУРАШБЕКОВ О.Б. ПРОБЛЕМЫ ВНЕДРЕНИЯ СОВРЕМЕННЫХ СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ СТАНОВЛЕНИЯ НАЦИОНАЛЬНОЙ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ РЕСПУБЛИКИ КАЗАХСТАН .....	240

*Верстка:*  
Ж.Ш. Тлегенова  
К.Н. Саратекова

Отдел организации научно-исследовательской  
и редакционно-издательской работы Алматинской академии  
МВД Республики Казахстан имени Макана Есбулатова  
050060 Алматы, ул. Утепова, 29

Подписано в печать 29 июня 2020 г.  
Формат 60x84 <sup>1</sup>/<sub>16</sub> Бум. тип. №1. Печать на ризографе.  
Уч.-изд. л. 10,9. Тираж 100 экз.