



ОТКРЫТАЯ НАУКА  
издательство

Международный журнал информационных технологий и  
энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.9

## ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

**Хитев А. П., Шиков И. В.**

*Владимирский юридический институт Федеральной службы исполнения наказания России, Владимир, Россия (600020, г. Владимир, ул. Б. Нижегородская, 67е), e-mail: hitevap@mail.ru*

**В России компьютерная криминалистика не имеет широкого распространения, что снижает качество расследования кибератак. С появлением облачных технологий, цифровая криминалистика столкнулась с объективно существующими проблемами. Для решения поставленной проблемы необходимо уделять особое внимание развитию науки компьютерной криминалистики, установлению стандартов деятельности при расследовании таких преступлений и повышению компьютерной грамотности населения.**

Ключевые слова: Компьютерная криминалистика, специалист, кибератака, киберпреступление, информация, цифровизация.

## PROSPECTS FOR THE USE OF INFORMATION TECHNOLOGY IN THE DETECTION AND INVESTIGATION OF CRIMES

**Khitev A. P., Shikov I. V.,**

*Vladimir Law Institute of the Federal Penitentiary Service of Russia, Vladimir, Russia (600020, Vladimir, B. Nizhegorodskaya st., 67e), e-mail: hitevap@mail.ru*

**In Russia, computer forensics is not widely used, which reduces the quality of cyberattack investigations. With the advent of cloud technologies, digital forensics has faced with objectively existing problems. To solve this problem, it is necessary to pay special attention to the development of computer forensics science, the establishment of standards for the investigation of such crimes and the improvement of computer literacy of the population.**

Keywords: Computer forensics, specialist, cyberattack, cybercrime, information, digitalization.

В век информационных технологий, проблема кибербезопасности приобрела особое значение. Компьютерные науки с каждым годом выходят на новый уровень развития, технологии совершенствуются и внедряются в повседневную жизнь, сохраняя все данные о пользователе. По этой причине человек начинает задумываться о безопасности собственной информации. Однако технологии злоумышленников также «не стоят на месте», и как следствие совершаются киберпреступления нового масштаба.

Оптимизация расследования – это проблема, которая постоянно стоит перед теорией криминалистики. Она обусловлена практикой установления обстоятельств совершения преступлений. То, насколько успешно данная проблема будет разрешена, во многом зависит от средств, которые используются в ходе расследования.

В России компьютерная криминалистика не имеет широкого распространения, что снижает качество расследования кибератак. Так, при расследовании взлома квартиры, следователь имеет чёткое понимание поэтапности своих действий. Поступил звонок, выезд на место преступления, осмотр места преступления, сбор вещественных доказательств, допрос потерпевших и свидетелей и т.п. При расследовании преступлений, связанных с хищением денежных средств с расчетных счетов или персональных данных, обнародованием порочащей честь и достоинство граждан информации, необходимы специальные знания порядка возникновения и движения информации в киберпространстве. В такой момент расследование становится невозможным без специалиста-форензика.

Возникновение информационной среды способствовало возникновению цифровой следовой информации, позволяющей не только расследовать и раскрывать преступления, но и пресекать совершения возможных преступлений, таким примером может служить АИС «Безопасный город» и интегрированных в нее подсистем, видеофиксации, геопозиционирования и др. Создаваемые на основе этой системы центры обработки и хранения информации позволяют выявлять и пресекать преступления [2, с. 150].

Эволюция способов совершения преступлений и орудий преступлений не всегда требует эволюции науки криминалистики и появления ее разновидностей. Надо просто оценить перспективы экстраполяции способов и методик доказывания обстоятельств совершения преступлений в эпоху цифровизации общественных отношений с точки зрения положений современной криминалистики и всего криминального научного блока. Вместе с тем криминалистика признает наличие такой науки, как информатика, под которой понимается техническая наука, систематизирующая приемы создания, хранения, обработки и передачи информации средствами электронно-вычислительной техники, а также принципы функционирования этих средств и методы управления ими.

За рубежом во многих англоязычных странах она также называется computer science – компьютерная наука. Теоретической основой информатики является группа фундаментальных наук, основанных на физике и высшей математике [1, с. 19].

В Российской Федерации, с появлением облачных технологий, цифровая криминалистика столкнулась с объективно существующими проблемами. Несмотря на имеющиеся немногочисленные исследования по цифровой криминалистике в облачных структурах, эта тема все еще в значительной степени не исследуется, и ученым предстоит проделать огромный объем работы [3, с. 75].

В настоящее время количество составленных нормативных правовых актов и научных доктрин об информации и её защите недостаточно для достижения поставленных целей в области обеспечения информационной безопасности. Для решения данной проблемы необходимо составить методические рекомендации, которые будут подробно описывать действия следователей и специалистов в различных областях науки и техники при расследовании киберпреступлений с учётом их вариативности.

Кроме того, необходимо сформировать максимально возможный список преступлений, связанных с движением информации в компьютерном пространстве, сгруппировав их по схожим признакам и индивидуальным особенностям.

Первоначальные действия специалиста должны быть связаны с собиранием и сохранением имеющихся данных, классификацией противоправных деяний, оценкой ущерба

и оставшихся потенциальных рисков. В зависимости от вида преступления способ и объем указанных данных будет отличаться.

Необходимо помнить, что сведения, полученные с компьютера нематериальны, а значит привычные следователям варианты раскрытия преступлений в большинстве случаев будут неэффективны. После чего, необходимо определить круг лиц, который имел доступ к объекту защиты информации, а также перекрыть потенциальные каналы утечки информации, обезопасив оставшиеся данные.

Следующим этапом является анализ полученных сведений, а также моделирование ситуации и восстановление хронологии событий по зафиксированным сохраненным данным с использованием специальных ПО (например: AccessDataForensicToolkit, BrowserForensicTool, EncryptedDiskDetector и т.д.). Набор базовых программ также необходимо отразить в специальной документации. Последующие действия связаны непосредственно с установлением лица, совершившего преступление, которое будет проходить по индивидуальной схеме в зависимости от киберпреступления.

Актуальность проблемы компьютерной криминалистической методики указывает на необходимость развития области компьютерной криминалистики на документальном и официальном уровне. Преимуществом создания предложенных документов является универсальность данного порядка действий. Общая последовательность действий для криминалиста будет актуальна и полезна для каждого преступления.

Постоянное улучшение методов кибератак и повышение квалификации криминалистов требует постоянного обновления и дополнения нормативных правовых документов, для поддержания уровня и продолжения раскрытия усовершенствованных киберпреступлений.

Постоянного развития сферы компьютерной криминалистики на документальном уровне недостаточно для повышения уровня развития форензики в России. Необходимым дополнением является введение новых предметов при обучении криминалистов и следователей или добавление новой специальности.

Таким образом, при росте совершаемых в век информационных технологий преступлений, связанных с движением информации в компьютерном пространстве, усложнение алгоритмов вредоносных программ, отсутствие достаточного количества нормативных правовых и научных источников, закрепляющих поэтапный и подробный ход расследования таких преступлений, существенно влияет на предотвращение и раскрываемость последних. Для решения поставленной проблемы необходимо уделять особое внимание развитию науки компьютерной криминалистики, установлению стандартов деятельности при расследовании таких преступлений и повышению компьютерной грамотности населения.

В заключении хочется еще раз подчеркнуть, что обеспечения безопасности общества является приоритетной задачей, как государства в целом, так и правоохранительных органов в частности, построение правового общества и государства не возможно, без контроля над преступностью и неотвратимости наказания. А информационные технологии способны стать теми информационно-технологическими средствами, которые облегчат достижения задач по раскрытию расследованию преступлений и станут теми инструментами, теми драйверами модернизации процессов профилактики и борьбы с преступностью.

Учитывая специфику облачных структур, для всего мирового сообщества, вовлеченного в цифровизацию, видится целесообразным интеграция научных криминалистических знаний, накопленных в РФ с целью:

- разработки специальных юридических средств и методов, регулирующих сферу предоставления облачных услуг;
- разработки и введения общего международного стандарта для развертывания и функционирования облачных инфраструктур, обеспечивающего возможность криминалистического сбора информации в соответствии с тремя компонентами, описанными выше;
- введения стандартов по применяемым инструментам и методам, используемым в цифровой криминалистике, с целью не допустить исключения собранных доказательств в суде;
- обмена практическими рекомендациями, выполненными исследователями, с целью развития и совершенствования применяемых криминалистических средств и методов.

В этой связи, безусловно, необходимо внедрение передовых достижений науки и техники в цифровую криминалистику, которая постепенно занимает лидирующие позиции в раскрытии и расследовании преступлений во всем мире.

Таким образом, актуальность цифровой криминалистики и разработка ею различных методов в целях раскрытия, расследования и предупреждения преступлений с каждым годом будет увеличиваться. Это обусловлено тем, что цифровизация проникает во все сферы человеческой жизни.

### Список литературы

1. Кучин О.С. К вопросу о дефиниции «цифровая криминалистика» // Современные технологии и подходы в юридической науке и образовании: Сборник 157 материалов международного научно - практического форума, Калининград, 2021. С. 19.
2. Морозова Н.В. Криминалистические методики расследования преступлений. Основания и принципы формирования // Закон и право. 2020. № 8. С. 150.
3. Шевченко А.С. Методы цифровой криминалистики в расследовании преступлений // Современные вызовы и перспективы развития молодежной науки. 2021. С. 75.

### References

1. Kuchin O.S. On the question of the definition of "digital forensics" // Modern technologies and approaches in legal science and education: Collection of 157 materials of the international scientific and practical forum, Kaliningrad, 2021. p. 19.
  2. Morozova N.V. Forensic methods for investigating crimes. Foundations and principles of formation // Law and law. 2020. No. 8. p. 150.
  3. Shevchenko A.S. Digital Forensics Techniques in the investigation of crimes // Modern challenges and prospects for the development of youth science. 2021, p. 75.
-