Э. Ю. Латыпова,
кандидат юридических наук, доцент,
Казанский инновационный университет имени В. Г. Тимирясова
Р. Р. Мусина,
заместитель декана юридического факультета
по научной и воспитательной работе,
Казанский инновационный университет имени В. Г. Тимирясова
Э. М. Гильманов,
старший преподаватель кафедры уголовного права и процесса,
Казанский инновационный университет имени В. Г. Тимирясова

ЦИФРОВЫЕ ТЕХНОЛОГИИ В РАССЛЕДОВАНИИ ЭКОНОМИЧЕСКИХ ПРЕСТУПЛЕНИЙ

Аннотация. В настоящее время одним из самых инновационных направлений в расследовании преступлений является использование различного рода цифровых технологий. Существенное место среди всех преступлений занимают преступления против собственности, часть из которых может совершаться с использованием цифровых технологий. В то же время и при расследовании экономических преступлений также активно применяются цифровые технологии. В представленном материале анализируются особенности расследования некоторых экономических преступлений с учетом использования отдельных цифровых технологий. Полагаем, что перспективы использования цифровых технологий в криминалистике при расследовании отдельных видов преступлений являются поистине прорывными!

Ключевые слова: экономические преступления, цифровизация, цифровые технологии, расследование преступлений

DIGITAL TECHNOLOGIES IN THE INVESTIGATION OF ECONOMIC CRIMES

Abstract. Currently, one of the most innovative areas in the investigation of crimes is the use of various kinds of digital technologies. A significant place among all crimes is occupied by crimes against property, some of which can be committed using digital technologies. At the same time, digital technologies are also actively used in the investigation of economic crimes. The presented material analyzes the features of the investigation of some economic crimes, taking into account the use of certain digital technologies. We believe that the prospects for the use of digital technologies in criminology in the investigation of certain types of crimes are truly breakthrough!

Keywords: Economic crimes, Digitalization, Digital technologies, Crime investigation

Введение. Генеральная прокуратура Российской Федерации ежегодно фиксирует рост преступлений, совершаемых с использованием цифровых технологий. Соответственно, необходимо использовать указанные технологии и при расследовании совершенных с их применением преступлений.

Актуальность темы напрямую вытекает из приоритетов распространения и использования информационных технологий в социально-экономической среде.

Среди цифровых технологий, применяемых при расследовании экономических преступлений, одним из первых является использование современных цифровых камер. Однако спектр их применения может быть более широким [3. С. 264], чем просто фиксация какого-либо изображения.

Динамика использования цифровых технологий при расследовании преступлений, в том числе экономической направленности, повышается с возникновением новых информационно-телекоммуникационных технологий, а также с появлением и внедрением новейшего высокотехнологичного оборудования и возможностями использования искусственного интеллекта [1].

Основная часть. Мошенничество с помощью методов социальной инженерии практически не оставляет клиентам банков (особенно их виртуальных представительств) шансов вернуть деньги обратно, на свой банковский счет. Такая ситуация возникает в случае, если лицо под влиянием обмана само совершает определенную банковскую операцию, либо самостоятельно разглашает данные, позволяющие ее провести [8. С. 108]. В таком случае банковская карта будет считаться скомпрометированной, что приводит к ситуации, когда кредитные организации не будут нести никакой ответственности за пропажу с нее денежных средств. Заметим, что пункт с подобным содержанием считается стандартным для обычных банковских договоров. Соответственно, раскрыть такое преступление также чрезвычайно сложно, хотя количество потерпевших от таких мошенничеств постоянно растет.

Необходимо учитывать, что каждый государственный орган в настоящее время должен вести в электронной форме соответствующие реестры, по которым заинтересованные лица могут получить необходимую информацию (например, можно проверить выданную доверенность и условия ее действия на сайте Федеральной нотариальной палаты и т. п.).

В последнее время в судебной и следственной практике достаточно часто встречаются случаи так называемого виртуального вымогательства, которое становится массовым явлением с большим количеством потерпевших, однако данный вид вымогательства имеет значительную латентность, так как жертвы опасаются обращаться в полицию из-за боязни огласки компрометирующей информации [6. С. 38] и общественного порицания своего поведения.

Так, на брифинге, посвященном работе Главного следственного управления МВД по РТ, первый заместитель начальника ГУ МВД по РТ М. Фролова сообщила, что 30-летняя преподавательница вуза из Казани отдала 2,8 млн рублей брачному аферисту, заложив квартиру, так как он угрожал разместить ее интимные фотографии на сайте вуза, чтобы они не попали в сеть Интернет [5]. К сожалению, сам факт задержания вымогателя, использующего виртуальный шантаж, вовсе не гарантирует привлечение данного лица к уголовной ответственности, так как в подавляющем большинстве случаев либо уголовное дело не возбуждается, либо ранее возбужденное дело прекращается по разным основаниям и передается в архив. Считаем необходимым в этой связи усилить контроль со стороны органов прокуратуры как за оперативно-розыскной деятельностью, так и за производством дознания и предварительного расследования в части оснований для прекращения уголовного дела по разным основаниям [6. С. 113].

Одним из достаточно традиционных в последнее время является использование при расследовании преступлений цифровых фотокамер, которые позволяют фиксировать изображение с достаточно большим разрешением, что в дальнейшем можно использовать при увеличении данного изображения. Оптимальный режим фотосъемки, по верному замечанию А. С. Волкова, позволяет получить фотоизображения следов рук с достаточной резкостью для назначения идентификационной дактилоскопической экспертизы по фотоизображению следов рук, полученных, например, с денежной купюры посредством использования паров йода, который в дальнейшем испаряется, делая затруднительным дальнейшее использование данных следов [3. С. 124]. Аналогичные действия можно произвести и на других финансовых документах, получая необходимую доказательную базу.

Использование при совершении преступлений поддельных документов также во многом объясняется высоким качеством таких подделок вследствие использования современной копировально-множительной техники, что весьма осложняет раскрытие и расследование преступлений, так как зачастую индивидуальные идентификационные признаки отсутствуют или являются очень незначительными.

По мнению О. А. Соколовой, весьма перспективным направлением установления давности следов пальцев рук является метод лазерной флюорографии (флюоресценции), основанный на различии в цвете люминисценции следов в зависимости от времени их оставления [10. С. 96]. Такие следы можно фотографировать методом цветоделительной съемки с использованием различных светофильтров; более того, потожировое вещество следа не разрушается, и его можно использовать для других методов исследования.

Как отмечается Н. Р. Шевко, «Татарстанская прокуратура в 2016 г. практически стала главным органом по надзору за исполнением провайдерами всей России судебных решений по блокировке запрещенных сайтов. Президент РФ Владимир Путин подписал поручения о разработке в стране системы мониторинга информационных угроз. Тем временем аналог таковой уже был разработан в Татарстане – эту работу проводила прокуратура РТ, выявляя и блокируя доступ пользователям к материалам пяти категорий, включая экстремизм и терроризм» [12. С. 104].

Система контроля противозаконных материалов ICM появилась в Татарстане в 2016 г. С ее помощью было выявлено более 18 тыс. сайтов, содержавших ссылки и цитаты на материалы из реестра экстремистских материалов Минюста РФ и признаки нарушения федерального законодательства. Проверкой этого контента занимались 17 прокуроров (сотрудники центрального аппарата прокуратуры РТ, а также прокуратур Казани, Апастово, Нижнекамска и Челнов), по решению которых одним нажатием кнопки были направлены на блокировку данные о 1 670 сайтах для потребителей наркотиков, 1 153 онлайн-казино, 945 сайтах по пропаганде суицида и 577 сайтах с детской порнографией [12. С. 104].

Используя сервер ICM, можно проводить оперативно-розыскные мероприятия, блокировать деньги на счетах или номера телефонов, и даже задерживать преступников. Соответственно, возможна борьба не только с распространением определенной информации, но и нанесение «удара» по самой инфраструктуре.

Таким образом, к цифровым технологиям расследования преступлений, помимо вышеперечисленных, можно отнести технологии восстановления и обнаружения

данных, собирание доказательств, криминалистический анализ цифровых средств и данных, необходимых для раскрытия и расследования преступлений [11, с. 164], включая сбор, хранение, анализ и представление данных, полученных любыми устройствами, фиксирующими информацию в цифровой сфере, вплоть до использования при расследовании преступлений искусственного интеллекта [2. С. 65].

Заключение. Практически единственным действенным способом предотвращения совершения экономических преступлений видится повышение информированности населения об опасности передачи различного рода информации (особенно коммерческого характера) посторонним лицам и возможности использования такой информации в противоправных целях. В среде несовершеннолетних возможно проведение лекций о безопасном поведении в сети Интернет, с целью повышения их информированности о нежелательности подобных действий.

Эффективным способом противодействия подделке документов может являться повсеместное введение электронного документооборота, так как обычные бумажные документы легко подделать с помощью современных копировально-множительных аппаратов.

Глобализация информационных телекоммуникационных процессов приводит к выходу экономических преступлений за границы территории России, закрепляя их международный и даже транснациональный характер, не ограничивая территорией отдельного государства и повышая их общественно опасный характер.

Список литературы

1. Бегишев И. Р., Латыпова Э. Ю., Кирпичников Д. В. Искусственный интеллект как правовая категория: доктринальный подход к разработке дефиниции // Актуальные проблемы экономики и права. 2020. Т. 14, № 1. С. 79–91.

2. Белова М. А. Использование искусственного интеллекта в расследовании преступлений / В сборнике: Цифровые трансформации в развитии экономики и общества. Материалы XVIII Международной научно-практической конференции. В 4-х томах. Воронеж, 2021. С. 65–69.

3. Волков А. С. Применение цифровых технологий в ходе расследования преступлений в экономической сфере // Экономическая безопасность и качество. – 2018. № 2 (31). С. 124–126.

4. Гильманов Э. М., Кирпичников Д. В. О необходимости разработки методики расследования преступлений в сфере обращения цифровой информации // Актуальные проблемы государства и права. 2020. Т. 4, № 14. С. 262–277.

5. Кривопатре Е. На уловки 32-летнего многократно судимого за разбои и грабежи жителя Казани попались три жительницы Татарстана // https://www.tatar-inform.ru/news/2019/04/03/647114/ (дата обращения: 01.09.2022).

6. Латыпова Э. Ю. Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Oeconomia et Jus. – 2019. – № 2. – С. 35–45.

7. Латыпова Э. Ю., Ключникова К. Е. Проблемы уголовной ответственности за вымогательство с использованием виртуального шантажа / Информационные технологии в деятельности органов прокуратуры. Сборник материалов II Всероссийской научно-практической конференции. Казань, 2019. С. 110–113.

8. Латыпова Э. Ю., Мусина Р. Р. Некоторые проблемы мошенничеств с помощью использования банковской карты с голосовым помощником / Информационные технологии в деятельности органов прокуратуры. Сборник материалов II Всероссийской научно-практической конференции. Казань, 2019. С. 107–109.

9. Мусина Р. Р. К вопросу о развитии уголовной ответственности за преступления против собственности в законодательстве России // Oeconomia et Jus. 2019. № 1. С. 64–72.

10. Соколова О. А. Использование результатов диагностических экспертиз по следам человека в уголовном судопроизводстве // Вестник Московского университета МВД России. 2019. № 1. С. 94–98.

11. Соловьева С. М. Применение цифровых технологий в криминалистике // Молодой ученый. 2019. № 51 (289) С. 161–164.

12. Шевко Н. Р. Информационные технологии в деятельности прокуратуры: преимущества и недостатки / В сборнике: Информационные технологии в деятельности органов прокуратуры. Сборник материалов II Всероссийской научно-практической конференции. Казань, 2019. С. 102–106.

О. И. Лепешкина,
кандидат юридических наук, доцент,
Северо-Западный институт управления – филиал Российской академии
народного хозяйства и государственной службы
при Президенте Российской Федерации

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РОССИИ

Аннотация. Целью исследования является определение основных направлений реализации государственной политики в области противодействия киберпреступности, а также обозначение перспективы развития ее нормативного правового регулирования. В настоящее время нет единого международного правового механизма противодействия киберпреступности, имеющей транснациональный характер, что затрудняет сотрудничество государств в данной области, развитие и унификацию национального законодательства. Автором сделан вывод о необходимости принятия Стратегии кибербезопасности, Закона «О противодействии киберпреступности» и соответствующей государственной программы.

Ключевые слова: цифровые технологии, киберпреступность, киберпреступление, противодействие киберпреступности, высокотехнологичная преступность, компьютерные преступления, кибербезопасность, киберпространство

THE PRINCIPAL DIRECTIONS OF ANTI-CYBERCRIME IN RUSSIA

Abstract. The goal of this article is to define the principal directions of anti-cybercrime in realization of anti-cybercrime state politics, and also to mark perspectives it's law regulation. There is not the international law mechanism of anti-cybercrime in this time. Therefore, there is difficulty of international collaborate with states about anti-