но ограничивается самим пунктом пропуска. В то же время весь пункт пропуска не является объектом осмотра места происшествия и видится целесообразным его территориально ограничивать тем местом, где подложный документ был выявлен. Поскольку в пунктах пропуска подложные документы выявляются в тех местах, где проверяются документы у физических лиц, пересекающих государственную границу, военнослужащими подразделений пограничного контроля, то и объектом осмотра места происшествия соответственно будет являться их рабочее место, т. е., как правило, кабина (модуль) паспортного контроля (в зависимости от технологических возможностей конкретного пункта пропуска, где был выявлен подложный документ). В то же время проведение осмотра места происшествия именно в той кабине (модуле) паспортного контроля, где непосредственно был выявлен подложный документ, является достаточно проблемным, поскольку процесс проверки документов в пункте пропуска не прекращается в течение суток. Данное обстоятельство наряду с отсутствием единого методологического подхода к проведению осмотров в пунктах пропуска через государственную границу может приводить к формализму в его проведении и допускаемым ошибкам. Все это предопределяет необходимость соблюдения следующих предлагаемых методических рекомендаций по проведению осмотра места происшествия в пунктах пропуска через Государственную границу Республики Беларусь:

1) протокол осмотра места происшествия в обязательном порядке должен содержать прилагаемую к нему таблицу фотоснимков;

2) данная таблица фотоснимков должна содержать:

ориентирующую фотографию пункта пропуска. При этом на фотоснимке должно быть видно название пункта пропуска, в котором проводится осмотр места происшествия;

обзорную фотографию кабины (модуля) паспортного контроля или другого места выявления подложного документа снаружи;

минимум две обзорные фотографии обстановки внутри кабины (модуля) паспортного контроля, выполненные с противоположных сторон;

обзорную фотографию рабочего места контролера, где был выявлен подложный документ. При этом на данной фотографии должен просматриваться тот подложный документ, который был выявлен;

минимум два детальных, выполненных по правилам масштабной фотосъемки фотоснимка выявленного документа (общего вида обложки и страницы с установочными данными владельца документа);

3) проведение осмотра места происшествия должно выполняться при обязательном участии понятых и желательно при участии специалиста,



в качестве которого в пункте пропуска можно привлекать военнослужащего подразделения специальной проверки документов;

4) в протоколе осмотра места происшествия указываются те технические средства, которые непосредственно применялись в ходе осмотра. К ним обязательно относятся средства фотографирования (с указанием марки и модели фотоаппарата или телефона, а также карты-памяти, на которую осуществлялась запись) и измерения.

Следует обратить внимание на минимальный характер представленных методических рекомендаций, что предопределяет необходимость дальнейшей их разработки в целях повышения качества проводимых следственных действий в пунктах пропуска через Государственную границу Республики Беларусь. Все вышеизложенное обусловлено важностью рассматриваемой проблемы в контексте оптимизации деятельности правоохранительных органов по раскрытию и расследованию преступлений, совершаемых на государственной границе белорусского государства.

УДК 343.9

***А.В. Маилян***

## ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Цифровизация всех сфер общественной жизни заключает в себе как положительные, так и отрицательные аспекты. Компьютеризация жизнедеятельности населения сформировала перед правоохранительными органами совершенно новую категорию преступлений – преступлений в сфере IT-технологий. К ним мы можем отнести и преступления, совершенные в сфере компьютерной информации. Основная трудность расследования данных преступлений заключается в усложненном процессе сбора доказательств по уголовным делам. Этот этап выступает основополагающим в ходе раскрытия преступлений, так как вся деятельность следователя и дознавателя направлена на получение сведений, имеющих значение для уголовного дела.

На сегодня мы можем выделить ряд следующих проблемных вопросов, возникающих на стадии предварительного расследования:

1. Трудности в обнаружении лица, совершившего преступление.

Это связано с тем, что преступники применяют специальные средства, позволяющие сокрыть местонахождение устройства, с которого осуществлялся вход в компьютерную систему. Сложность обнаружения

субъекта преступления. Однако, даже вычислив расположение устройства, правонарушитель может использовать серверы, с помощью которых будут скрыты все сведения, идентифицирующие его личность. В связи с этим установление и выявление виновного, а значит, и осуществление правосудия, становится достаточно трудной задачей.

2. Трудности в фиксации и обнаружении цифровых следов.

В связи с тем что цифровые следы имеют краткосрочный характер, зафиксировать их как признак преступления становится невозможным. Помимо этого различные современные технологии способствуют при их неправомерном применении устранению цифровых доказательств совершения противоправного деяния.

3. Отсутствует необходимость личного контакта преступника с объектом преступления.

Правонарушение может совершаться субъектом преступления дистанционно. Этот фактор исключает возможность личного обнаружения преступника, так как за время вычисления его местонахождения он может немедленно скрыться или навести на ложный след. Преступник может находиться на достаточном расстоянии от места.

4. Уровень подготовки специалистов и материально-техническое обеспечение подразделений уголовного розыска.

Под компьютерной же информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Напомним, типичным преступлением, связанным с незаконным получением компьютерной информации, является преступное деяние, совершаемое сотрудниками кредитных учреждений и операторов мобильной связи.

В условиях распространения коронавирусной инфекции появились новые преступления, в том числе в сфере компьютерной информации. Так, Следственный департамент Министерства внутренних дел Российской Федерации расследует уголовное дело в отношении медсестры Б. (эпизодов 13). Медсестра незаконно вошла в федеральный реестр вакцин против COVID-19, куда внесла ложную информацию об иммунитете людей, использующих вакцины для профилактики COVID-19.

Одной из ключевых проблем в борьбе с преступностью в области компьютерной информации является сговор злоумышленников с целью использования так называемых альтернативных средств реальных IP-адресов для осуществления преступной деятельности. Причиной этого преступления может быть недостаточный уровень информаци-



онной безопасности предприятия, возможность несанкционированного доступа к компьютерной информации или распространения вредоносных компьютерных программ, а также низкая квалификация и способности персонала, ответственного за безопасность компьютерной сети охраняемой законом организации.

В связи с этим для достижения цели предотвращения необходимо соблюдать меры по исключению доступа третьих лиц к гаджетам граждан.

Для предупреждения преступности и повышения технической грамотности населения можно рекомендовать принять ряд мер:

1) разработка руководств, в зависимости от различного уровня просвещенности в данной сфере каждого пользователя [4, с. 78–84];

2) путем использования различных брошюр, памяток, прямых эфиров, видеороликов, сети Интернет и ее ресурсов, а в особенности через сайты и аккаунты социальных сетей правоохранительных органов распространить выработанные рекомендации (руководства);

3) обратить особое внимание на обучающихся школ и вузов, проводить и организовывать с ними круглые столы, беседы, встречи и другие мероприятия;

4) агитировать к этому направлению сайты и интернет-ресурсы в сфере компьютерных информационных технологий, компании и организации, производящие и продающие свою продукцию в данной сфере.

Такие меры помогут сократить количество преступлений и их негативных последствий в сфере компьютерной информации.

Резюмируя вышеизложенное, мы можем предложить следующий ряд мер, способствующих дальнейшему усовершенствованию методики раскрытия и расследования преступлений, совершенных в сфере компьютерной информации:

1. Конкретизировать правовую регламентацию, закрепленную в уголовном законодательстве, в целях выделения конкретных категорий преступления. Устранить коллизии и ясно отобразить в содержании сущность преступлений данной категории.

2. Проанализировать практику расследования цифровых преступлений и систематизировать деятельность в единый алгоритм действий, направленный на раскрытие преступления [2, с. 92–95].

Таким образом, цифровизация экономики и информатизация общества представляют собой мировой интеграционный процесс, который сопровождается переводом информации в компьютерное пространство.

Эта тенденция приведет к повышению производительности экономики как страны, так и всего мира. Однако всему процессу будет сопутствовать криминализация ранее неизведанных отраслей деятельно-

сти, с чем столкнутся законодательные и правоохранительные органы. Помимо угроз личной безопасности назреет вопрос национальной безопасности [3, с. 22].

Таким образом, освоение данной сферы общественной жизни будущими специалистами и сотрудниками полиции должно стать первоначальной задачей образовательных организаций.

В результате проведенного исследования мы приходим к следующим выводам:

1. Целесообразно повысить ответственность операторов связи и организаторов, распространяющих информацию в интернете, за нарушение требований законодательства, касающихся хранения, приема, передачи, доставки и (или) обработки голосовых сообщений, письменных текстов, изображений, звуков, видео- или иной электронной информации пользователей сети Интернет или пользователей услуг связи, на территории Российской Федерации, а также информации о содержании самой передачи.

2. Совершенствовать преобразование подразделений, участвующих в борьбе с преступлениями, с использованием информационно-коммуникационных технологий, оснащения их современным программным обеспечением и электронным взаимодействием технологии [1, с. 90–95].

3. Повысить уровень квалификации специалистов, осуществляющих расследование преступлений в сфере компьютерных технологий.

4. Проводить оценку и мониторинг раскрытых и нераскрытых преступлений данной категории.

5. Структурировать и закрепить единую классификацию каждого направления современных преступлений в сфере компьютерных технологий.

6. Проанализировать общую характеристику и индивидуальные признаки преступлений в целях составления пособия по расследованию уголовных дел в области информационно-коммуникационных технологий.

1. Потапов, С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации / С.А. Потапов // Соц.-экон. явления и процессы. – 2016. – Т. 11. – № 10. – С. 90–95.

2. Ефремов, К.А. Личность преступника, совершающего преступления в сфере компьютерной информации / К.А. Ефремов // Общество: политика, экономика, право. – 2016. – № 6. – С. 92–95.

3. Милашев, В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. ... канд. юрид. наук : 12.00.09 / В.А. Милашев ; Моск. гос. ун-т им. М.Ю. Ломоносова. – М., 2020. – 22 с.



4. Маилян, А.В. Особенности проведения допроса при расследовании хищений, совершенных с использованием электронных средств платежа / А.В. Маилян // Криминалистика: вчера, сегодня, завтра. – 2020. – № 3 (15). – С. 78–84.

УДК 343.983.22

***А.Н. Матлак***

## ДЕТАЛЬНЫЙ ОСМОТР ОГНЕСТРЕЛЬНОГО ОРУЖИЯ НА МЕСТЕ ПРОИСШЕСТВИЯ

Осмотр места происшествия является наиболее важным следственным действием, проводимым для обнаружения и первоначального исследования объектов-носителей криминалистически значимой информации.

Детальный осмотр огнестрельного оружия в ходе проведения осмотра места происшествия является основным элементом рабочего этапа указанного следственного действия и преследует следующие цели: осуществление необходимых измерений; обнаружение криминалистически значимой информации, включая следы рук, одежды, крови и т. п., на поверхности оружия; получение детальных фотоснимков оружия; определение конструктивных особенностей оружия (без разборки) с установлением наличия маркировочных обозначений и другой значимой для расследования преступления информации.

Детальный осмотр проводится только после приведения огнестрельного оружия в безопасное для участников следственного действия состояние (разряжание оружия либо разобщение его деталей и механизмов, препятствующее производству выстрела).

Для проведения детального осмотра оружия его кладут на чистую бумагу, обеспечивая при этом достаточную освещенность смотровой поверхности, чтобы исключить утрату любых отделившихся от оружия частиц.

Производство измерений является важным элементом фиксации огнестрельного оружия на месте происшествия, ведь для признания любого объекта вещественным доказательством и использования в дальнейшем по делу, в процессуальном документе (в данном случае в протоколе осмотра места происшествия) должны быть приведены исчерпывающие на первом этапе расследования данные об объекте, впоследствии только уточняющиеся при производстве судебной экспертизы. Для измерений необходимо использовать инструменты, прошедшие ежегодную государственную поверку в установленном законодательством порядке, чтобы исключить в дальнейшем возможные противоречия полученных