МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

РОССИЙСКОЕ ПРАВОВЕДЕНИЕ:
ТРИБУНА МОЛОДОГО УЧЁНОГО

Выпуск 19

Томск
Издательский Дом Томского государственного университета
2019

на выявление таких сведений о личности указанного субъекта, как готовность к установлению контакта со следователем, общую коммуникабельность и т.д.[1]

Добавим, что названные операциональные тактико-криминалистические средства могут носить как исследовательский, так и обеспечительный характер. К числу проблемных следует отнести вопросы классификации тактико-криминалистических средств, построенной на основе их наиболее существенных свойств и позволяющей использовать те из них, которые в наибольшей мере соответствуют типичным следственным ситуациям.

ПЕРСПЕКТИВНЫЕ НАПРАВЛЕНИЯ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ ЦИФРОВЫХ СЛЕДОВ

А.В. Извеков, студент ТГУ
Научный руководитель – канд. юрид. наук, доцент И.С. Фоминых

Подобно тому, как в физическом мире мы оставляем следы после себя: отпечатки пальцев, волосы, волокна одежды, когда мы перемещаемся и взаимодействуем с людьми, местами и объектами, действия в цифровой сфере также оставляют цифровые следы. Это могут быть виртуальные фрагменты файлов, журналы активности, метки времени, метаданные и т.д. Все они могут быть очень ценными по ряду причин. Данные указания могут быть полезны в качестве доказательств при установлении происхождения документа или программного обеспечения при определении иных обстоятельств уголовного дела.

В результате объединения передовых технологий и интернета увеличилось как количество, так и изощренность киберпреступлений, нацеленных на финансовые учреждения и важнейшие инфраструктуры Российской Федерации. Сегодня криминальные тенденции демонстрируют рост использования фишинговых писем, захватов учетных записей, внедрение вредоносных программ, хакерских атак и сетевых вторжений, приводящих к утечкам данных.

Помимо выявления прямых доказательств преступления, цифровая криминалистика может использоваться для того, чтобы соотносить уже имеющиеся в деле доказательства с конкретным подозреваемым, подтверждать алиби или иные его заявления, определять намерения, идентифицировать источники (например, в случаях авторского права) или аутентифицировать документы. В связи с этим, тему статьи считаю особо актуальной в наши дни.

Правоохранительные органы играют ключевую роль в достижении информационной безопасности, расследуя широкий круг киберпреступлений от краж и мошенничества до эксплуатации детей. Федеральная служба безопасности сотрудничает как с внутренними структурами (СК, МВД, прокуратура), так и с внешними (Интерпол, Европол) для проведения расследований, в целях привлечения к ответственности киберпреступников. Следователи и эксперты по

[1] См.: Князьков А.С. Проблемы классификации тактических операций // Вестник Тюмен. гос. ун-та. 2012. № 3. С. 190.

сетевой безопасности, изучая новейшие технологии, имеющиеся в руках преступников, а также точки уязвимости систем безопасности, преследуют цель повышения эффективности расследования преступлений в информационной сфере.

Преступления, совершенные в электронном пространстве, стали чрезвычайно распространенным явлением в наши дни. Преступники используют технологии в совершении различных цифровых преступлений и создания новых проблем для сотрудников правоохранительных органов, адвокатов, судей, военных и специалистов в области безопасности.

По моему мнению, изучение деятельности и методологии киберпреступников, наряду с цифровым криминалистическим анализом используемых ими инструментов и способов, может дать представление о преобладающих или будущих тенденциях в области информационных атак, функционировании преступных сетей и новых видах вредоносных программ. Они могут внести значительный вклад в ресурсы знаний и передовой практики, а также в базы данных аналитики киберугроз.

Подводя общий итог, с уверенностью можно говорить о том, что цифровая криминалистика является междисциплинарной областью, охватывающей различные дисциплины, такие, как криминология, уголовно-процессуальное право, этика, компьютерная инженерия и информационно-коммуникационные технологии, информатика и судебная медицина. Следует отметить необходимость изучения теоретических основ следообразования, а также закономерности возникновения цифровых следов, отражающих механизм киберпреступления, с целью разработки предписаний по применению инновационных средств и специальных способов для обнаружения, изъятия и исследования виртуальных следов с целью раскрытия, расследования и предупреждения преступлений, совершенных с использованием киберсистем.

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА НЕЗАКОННОГО ОБОРОТА НАРКОТИЧЕСКИХ СРЕДСТВ ИЛИ ПСИХОТРОПНЫХ ВЕЩЕСТВ

С.В. Ионова, студентка НовГУ им. Я. Мудрого
Научный руководитель – канд. юрид наук, Н.В. Рязанова

Ни для кого не является секретом, что незаконный спрос на наркотические средства и психотропные вещества, рост их незаконного производства и оборота являются глобальной проблемой современности и представляет собой угрозу национальной безопасности всех государств.

Одной из основных причин распространения данной «индустрии» является появившийся с течением времени интерес к нашей стране со стороны государств, таких как Латинская Америка, регионов «Золотой треугольник» (Таиланд, Мьянмы, Лаос), где еще в середине XX века возникла система производ-