находится факультет подготовки специалистов в области информационной безопасности. «Подводя такой промежуточный итог работы факультета, я бы хотел отметить, что все-таки это решение по выработке технических компетенций практико-ориентированных и, безусловно, юридических. Поэтому данный факультет у нас является передовым и, безусловно, будет регулярно развиваться, регулярно совершенствовать образовательный процесс в рамках учебных дисциплин», – резюмировал он.

Кроме того, по мнению А. Тумакова, со временем цифровое право сформируется как отдельная отрасль. «Полагаю, что в настоящее время законодательство должно быть трансформировано. Причем трансформация должна происходить не только в области частного права, но и, безусловно, публичного права. Буквально вчера была поставлена задача Центральному банку и Министерству финансов предложить правовое регулирование цифровых финансовых активов. Думаю, что это достаточно позитивный пример, когда новые объекты, которые появляются в гражданском обороте, будут иметь соответствующее правовое регулирование. И, в целом, без выстраивания определенного категориального аппарата, в том числе в частном праве, нашим правоприменителям, судьям в том числе, достаточно сложно заниматься правоприменительной практикой, – добавил он. – Поэтому, полагаю, что законодательство в области как частного права, так и публичного права, должно трансформироваться в современных условиях и отвечать новым вызовам».

В результате исследования обоснован и разработан подход к повышению качества подготовки специалистов в области подготовки «Информационная безопасность».

УДК 343.98

И.О. Щербаков

ОСМОТР КОМПЬЮТЕРНЫХ УСТРОЙСТВ ПРИ РАССЛЕДОВАНИИ КИБЕРПРЕСТУПЛЕНИЙ

Несмотря на понижение темпа роста киберпреступлений, нельзя не отметить, что в целом все киберпреступления постоянно видоизменяются и совершенствуются, что снижает эффективность по их выявлению, раскрытию и расследованию. Развитие преступной среды предопределяет возможность обезличивания злоумышленников, а также совершение таких преступлений дистанционно, что позволяет скрыть

следы. В связи с этим растет уровень совершаемых рассматриваемых преступлений, поэтому деятельность правоохранительных органов во многом сейчас направлена на выявление, раскрытие и расследование преступлений, совершенных с использованием интернет-технологий.

Производство любого следственного действия, а особенно осмотра компьютерной техники, требует тщательной подготовки, обусловленной особенностями компьютерных средств. Осмотр электронных носителей информации возможно проводить в ходе осмотра места происшествия, либо как отдельное следственное действие [1].

На подготовительном этапе данного следственного действия следует:

проанализировать и систематизировать все сведения, имеющиеся в материалах уголовного дела, для определения вектора поиска криминалистически значимой информации;

привлечь специалиста, у которого есть необходимые компьютерно-технические средства;

разрешить вопрос об участии понятых, либо о применении технических средств, фиксирующих ход производства осмотра компьютерного устройства. Учитывая длительность и специфику производства данного следственного действия, целесообразным будет применение технических средств, что не противоречит ч. 1.1 ст. 170 Уголовно-процессуального кодекса Российской Федерации.

Для рабочего этапа характер осмотра методом «от общего к частному», т. е. сначала осматриваются внешние признаки устройства (цвет, марка, модель), а потом производится осмотр информации, содержащейся на электронном носителе. Неизменность, подлинность и сохранность источника информации обеспечивается следующим алгоритмом действий:

применять средства и программные обеспечения блокировки записи цифровой информации, копирования данных, позволяющих создавать копию, соответствующую оригиналу по содержанию и технологическим свойствам, позволяющие извлечь и проанализировать данные из устройств и облачных сервисов, такие как контакты, сообщения, звонки, геолокация, восстанавливают удаленные данные и др. [2];

не производить отключения уже запущенных программ и приложений, «авиарежима»;

не позволять самостоятельно совершать манипуляции с компьютерным устройством, если неизвестно, к какому результату это приведет;

детальный осмотр данных как на электронном устройстве, так и в «облачных» хранилищах;

удостоверение факта производства определенных действий, производимых с устройством, путем их фиксации письменно в протоколе,

составления фототаблицы, прилагаемой к осмотру, а также используя встроенную функцию на устройстве «скриншот».

На заключительном этапе оформляется протокол осмотра предметов и решается вопрос о дальнейшем хранении электронных устройств. Сведения, подлежащие занесению в протокол данного следственного действия:

1) осматриваемое устройство, его модель, марка, производитель, размеры, цвет, наличие внешних разъемов;

2) состояние устройства в момент осмотра, включенное либо выключенное;

3) провода, через которые производится электропитание прибора, их размер и цвет;

4) общее состояние осматриваемых устройств, внешний вид и наличие повреждений;

5) порядок соединения устройств с другими техническими средствами;

6) наличие или отсутствие вредоносных программ, их название, а также наличие или отсутствие антивирусной программы;

7) содержание найденной информации, откуда была скопирована [3].

Далее устройство упаковывается с соблюдением условий, исключающих возможность доступа к содержимому и дистанционного считывания.

Своевременное обнаружение компьютерных средств и правильное их изъятие предопределяет эффективность последующей компьютерно-технической экспертизы, назначаемой с целью извлечения информации, хранящейся на магнитных носителях, и обнаружения таким образом указанных следов преступной деятельности.

Список использованных источников

1. Иванов, В.Ю. К вопросу совершенствования противодействия киберпреступлениям правоохранительными органами / В.Ю. Иванов // Соврем. наукоем. технологии. – 2019. – № 1. – С. 52–57.

2. Бахтеев, Д.В. Криминалистическое мышление и программирование расследования / Д.В. Бахтеев // Вестн. Балт. федер. ун-та им. И. Канта. Сер. «Гуманитар. и обществ. науки». – 2018. – № 3. – С. 13–20.

3. Виноградова, О.П. Современные направления использования информационных технологий в раскрытии и расследовании преступлений / О.П. Виноградова // Тенденции развития современного уголовно-процессуального законодательства Российской Федерации : сб. науч. тр. Всерос. науч.-практ. конф. – Екатеринбург, 2019. – С. 24–28.

УДК 343.9

Л.Ю. Югай

НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ В ПРОТИВОДЕЙСТВИИ ПРЕСТУПНОСТИ: ОПЫТ РЕСПУБЛИКИ УЗБЕКИСТАН

Цифровая трансформация общества и государства влечет за собой динамичный рост сфер жизнедеятельности человека, где используются биометрические технологии. В Республике Узбекистан биометрическая идентификация личности используется в нотариальной деятельности, при оказании государственных и банковских услуг в удаленном режиме, при проведении вступительных экзаменов в высшие учебные заведения, при оформлении административного протокола при нарушении правил дорожного движения и в других случаях.

Данная тенденция имеет место и в деятельности по раскрытию и расследованию преступлений, что обусловливает качественное изменение применяемых научно-технических средств и методов, а также переход от материальной формы вещественных доказательств в цифровую. Правоохранительными органами эффективно используются специализированные биометрические базы данных.

Анализ правоприменительной практики показывает, что с учетом внедрения аппаратно-программного комплекса «Безопасный город» с интеллектуальной системой видеонаблюдения значительно возросло количество проводимых портретных исследований: начиная с 2019 г. – на 2,3 %, в 2020 г. – на 172,9 %, в 2021 г. – на 258,3 %, включая идентификации по фотороботу, фотоизображениям лиц, идентификаций неизвестных лиц и видеоматериалам. Учитывая, что количество портретных экспертиз, проведенных с 2017 по 2021 г., увеличилось на 119,7 %, портретных исследований за указанный период достигло 311,3 %, следует отметить важность оснащения системами видеонаблюдения всех общественных мест в комплексе с технологией распознавания лиц.

С апреля 2022 г. осуществляет свою деятельность Центр единого оперативного управления ГУВД г. Ташкента (далее – Центр). В дежурной части данного Центра в круглосуточном режиме ведется мониторинг системы видеонаблюдения общественных пространств с использованием технологии распознавания лиц. При обнаружении человека, похожего на лицо, находящееся в розыске, искусственный