Отметим, что проблемы, касающиеся ошибок, допускаемых специалистами при их участии в осмотрах места происшествия, частично рассматривались Е. Р. Россинской, А. А. Аубакировой, Э. В. Лантухом, А. В. Репиным, Е. Б. Мельниковым. Тем не менее количество публикаций на тему данных ошибок значительно меньше количества работ, касающихся экспертных ошибок, допускаемых при проведении экспертиз. Ошибки криминалистических учетов и коллекций изучены в меньшей степени.

Анализ деятельности экспертов при участии в качестве специалистов в осмотрах мест происшествий показывает, что ими допускаются ошибки, касающиеся неизъятия объектов, находившихся в непосредственном контакте с преступником, качества фотосъемки, оформления таблиц фотоснимков, полноты и правильности фиксации в протоколе информации, сообщаемой следователю специалистом.

Анализом судебно-экспертной деятельности установлено, что сотрудники, осуществляющие ведение криминалистических учетов, не в полной мере владеют либо неправильно применяют на практике отдельные положения нормативных правовых актов, регламентирующих ведение криминалистических учетов. Также экспертами допускаются описки, орфографические ошибки, ошибки в расстановке и указании признаков объектов криминалистических учетов, неверное заполнение полей электронных форм при формировании криминалистических учетов.

С целью недопущения ошибок экспертами при их участии в качестве специалиста в осмотре места происшествия и других процессуальных действиях и оперативно-розыскных мероприятиях, а также при ведении криминалистических учетов и коллекций, необходимо углубленно изучить сущность данных ошибок, причины их допущения, рассмотреть вопросы их классификации и предупреждения, основываясь на существующих исследованиях, касающихся вопросов экспертных ошибок, и современной практике отдельных видов деятельности эксперта. Таким образом, ошибки, допускаемые экспертами в отдельных видах деятельности, требуют дополнительного внимания и, соответственно, всестороннего исследования.

Сотникова Е. А.

МЕХАНИЗМ СЛЕДООБРАЗОВАНИЯ В КИБЕРПРОСТРАНСТВЕ

Сотникова Евгения Алексеевна, студентка 4 курса Белорусского государственного университета, г. Минск, Беларусь, bakugafa@gmail.com

Научный руководитель: канд. юрид. наук, доцент Хлус А. М.

Специфичность совершения преступлений и, соответственно, механизма следообразования связана в первую очередь с особенностями киберпространства как нового пространства совершения преступлений.

Законодатель не дает определение понятия «киберпространство», однако в постановлении Совета Министров от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» закреплено

определение информационного пространства (область деятельности, связанная с созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание и собственно информацию). Киберпространство неразрывно связано с информационной составляющей. Внутри киберпространства происходит огромное количество информационных потоков, поэтому вполне целесообразно при понимании сущности киберпространства учитывать дефиницию информационного пространства.

Киберпространство не имеет географической определенности. Это связано с тем, что любой объект киберпространства занимает определенный объем, который, в свою очередь, не снижает скорости перехода к другим объектам, следовательно, объекты не отделены между собой физическим расстоянием.

Функционирование киберпространства опирается на определенную технологическую инфраструктуру (хабы, серверы, компьютеры и другое), однако местом обнаружения следов могут быть и нематериальные объекты (например, профили пользователей в социальных сетях, электронные платежные системы («Qiwi-кошелек», «Koronapay»)) и т. д.).

Обязательным субъектом киберпространства является человек-пользователь. Именно человек выполняет те или иные действия (например, запуск вредоносной программы), которые осуществляются в киберпространстве, и итоговая цель их функционирования совпадает с целью лица. Любые действия пользователя отражаются в киберпространстве, образуя специфическую группу следов. Подобная группа следов не относится ни к идеальным следам, ни к материальным, так как эти следы образовались в кибепространстве, доступ к которому возможен через техническую инфраструктуру. А сами следы являются результатом изменений информации и логических и математических операций с двоичным кодом, что говорит о цифровом характере следов. Соответственно, целесообразно называть подобные следы цифровыми. Ввиду своего цифрового характера возникает особая сложность образования следов: при совершении каких-либо действий в киберпространстве преобразовывается не только информация, но и код (преобразование, которое приводит к изменению формы информации в отражательном процессе при неизменности ее содержания).

Как уже было выше отмечено, при совершении определенных действий в киберпространстве необходим пользователь, само пространство и конечный объект, на который направлена цель пользователя. Пользователь, используя свой компьютер, запускает, например, вредоносную программу; в этом случае механизм следообразования носит материальный характер. Далее действие, осуществленное с компьютера лица, взламывает защиту. Это действие направлено на получение информации и представляет собой цифровое следообразование. Компьютер лица, запустившего программу, и конечный объект (компьютер жертвы) связаны информационно, т. е.

задействован код преобразования информации. Конечный объект будет содержать всю информацию о проникновении в систему, а компьютер лица, запустившего программу, – всю информацию о проникновении. Таким образом, образуются две группы следов – материальные и цифровые следы.

Согласно разработанным криминалистикой правилам следы должны изыматься вместе с объектами, на которых они расположены или их фрагментами (частями). Цифровые следы, находясь в киберпространстве, одновременно расположены в пространстве и на любом объекте технической инфраструктуры ввиду того, что доступ (независимо от того, санкционированный или нет) к подобным следам можно получить с любого устройства технической инфраструктуры (например, компьютера). Следовательно, у цифровых следов нет конкретного объекта – следоносителя, и цифровые следы могут находиться одновременно на разных устройствах, что говорит об отсутствии связи между местом совершения определенных действий и местом образования следов.

Таким образом, механизм цифрового следообразования неразрывно связан с особенностями самого киберпространства. Например, цифровой след имеет информационный и дискретный характер. В процессе следообразования в киберпространстве образуется две группы следов – материальные и цифровые. Первые возникают в связи с использованием технической инфраструктуры, вторые – в связи с информационными и кодовыми преобразованиями. Для образования цифровых следов необходимо три участника: пользователь (преступник) – киберпространство – пользователь (жертва). Цифровые следы не имеют привязки к объекту – следоносителю, следовательно и отсутствует конкретное физическое местонахождение подобных следов.

Стариков Е. В.

ЭТИКО-ПРАВОВОЙ ПОДХОД К СМЕРТНОЙ КАЗНИ

Стариков Егор Вячеславович ,студент 1 курса Белорусского государственного университета, г. Минск, Беларусь, starjow@yandex.by

Научный руководитель: канд. юрид. наук, доцент Орехова Е. П.

Исторически смертная казнь эволюционировала из “принципа Талиона”, который в свою очередь подразумевал “ока за ока, зуб за зуб”. В те времена, если человек не отомстил за совершенный ему вред, не восстановил справедливость, считалось позором для пострадавшего или родственника. С усилением роли государства функция наказания перешла к специальному государственному аппарату. Убиение (смертная казнь) стало публичным и обрело уголовный характер, исполнялось от имени государственной власти.

В Уголовном кодексе Республики Беларусь смертная казнь как одно из видов наказания предусмотрена в 13 статьях. Однако суды предпочитают назначать альтернативные варианты наказания, предусмотренные в данных статьях. Таким образом, смертная казнь как наказание существует еще с