Секция «10.2 Финансовая безопасность Российской Федерации в условиях новой реальности»

Проблемные аспекты криминалистического обеспечения расследования преступлений в финансово-экономической сфере, совершаемых с использованием компьютерных средств

Научный руководитель – Каменева Анна Николаевна

Братухина Арина Александровна
Студент (магистр)
Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Москва, Россия
E-mail: arina.bratukhina@yandex.ru

В настоящее время человечество вступает в новую эру своего развития, именуемую информационным обществом. В данных условиях вопросы информационной безопасности приобретают особую остроту, а борьба с угрозами в данной сфере становится все более актуальной.

Центральным элементом криминалистической характеристики преступлений, так или иначе связанных с применением компьютерных технологий, выступает характеристика средств их совершения, а именно – компьютерных программ. Существенной особенностью, которая подлежит учету при формировании методик расследования, является то, что арсенал таких средств включает не только специально разработанное вредоносное программное обеспечение, но и иные программные продукты, которые изначально не предназначены для противоправной деятельности.

В результате модификации легального программного продукта злоумышленник получает действенный инструмент для неправомерного вторжения в компьютерные системы. Реализуя блокировку доступа к данным либо нарушение их функциональности, преступник впоследствии выдвигает требования о передаче денежных средств за восстановление информационных ресурсов. Указанные деяния образуют состав мошенничества в сфере компьютерной информации, предусмотренный статьей 159.6 Уголовного кодекса Российской Федерации (далее – УК РФ).

Основная сложность состоит в необходимости четкого разграничения штатного функционала исходной программы и несанкционированных деструктивных компонентов, привнесенных преступником. В ходе экспертного исследования требуется не только зафиксировать факт блокировки или уничтожения данных, но и обосновать умышленный характер видоизменения программного кода, совершенного с криминальной целью, что предполагает анализ логики функционирования приложения, его сопоставление с эталонными дистрибутивами и выявление конкретных алгоритмов, обусловливающих недоступность информации. Задача существенно усложняется при применении злоумышленником методов шифрования вредоносных элементов, которые маскируют их под легитимные системные процессы.

Проблемы возникают также на этапе формулирования вопросов, которые выносятся на разрешение экспертизы. Следователь обязан корректно определить род и вид назначаемой экспертизы, а также поставить перед специалистом задачи, ответы на которые будут обладать доказательственным значением. Вопросы не должны ограничиваться простой констатацией факта блокировки; они призваны установить взаимосвязь между модификацией программы, действиями пользователя и наступившими вредоносными последствиями. Неточные либо неполные формулировки способны привести к получению заключения, фиксирующего лишь технические аспекты, но не отвечающего на основные вопросы уголовного дела о способе совершения преступления и причинно-следственных связях.

Следовательно, доказывание по уголовным делам о мошенничестве, совершенном с использованием модифицированного легального программного обеспечения, предъявляет повышенные требования к уровню технической компетентности сотрудников правоохранительных органов и судейского корпуса. Преодоление обозначенных трудностей видится в развитии методического обеспечения судебной компьютерно-технической экспертизы, ориентированного на анализ гибридных вредоносных средств, а также в повышении квалификации следователей в части корректной постановки технических заданий для экспертов [4, с. 205].

Анализ данных судебной статистики также подтверждает наличие прямой корреляции между следственными ошибками и увеличением числа оправдательных приговоров, а также прекращенных уголовных дел в рассматриваемой сфере. Суды, оценивая доказательства, полученные в цифровой среде, при обнаружении их недоброкачественности либо процессуальных нарушений в оформлении, вынуждены исключать такие материалы из доказательственной базы [2, с. 347]. Подобная ситуация не только нивелирует результаты работы оперативных подразделений, но и негативно отражается на общественном доверии к системе правосудия в условиях цифровой трансформации.

Существующее количество аккредитованных экспертных учреждений и квалифицированных специалистов в них в настоящее время не соответствует масштабам распространения киберпреступности. Представляется целесообразным создание межведомственных экспертно-аналитических центров, оснащенных современным оборудованием для углубленного анализа данных, извлекаемых не только с компьютеров, но и с устройств интернета вещей, из облачных хранилищ и зашифрованных каналов связи. Подобные центры могли бы обеспечивать методическую и практическую поддержку следственных групп на местах в режиме реального времени.

Кроме того, организация регулярных стажировок сотрудников следственных подразделений в профильных IT-компаниях (по аналогии с уже существующей практикой взаимодействия с «Лабораторией Касперского») обеспечит получение ими уникального практического опыта и понимания внутренней логики функционирования цифровых систем, что невозможно в полной мере сформировать в условиях аудиторного обучения.

Таким образом, применение легального программного обеспечения при совершении противоправных деяний в финансово-экономической сфере порождает комплекс серьезных проблем в рамках криминалистического обеспечения расследования. Основная сложность состоит в необходимости экспертного разграничения штатного (заложенного разработчиком) функционала программы и привнесенных в нее деструктивных модификаций.

Источники и литература

1) Клещина Е.Н. Проблемы и основные направления совершенствования правового регулирования противодействия киберпреступности // Государственная служба и кадры. 2024. № 4. С. 237-241.
2) Никульченкова Е.В. Проблемы противодействия киберпреступности в России // Психопедагогика в правоохранительных органах. 2023. № 3 (94). С. 345-351.
3) Ходанов А.И. О некоторых теоретических проблемах противодействия киберпреступности // Право и государство: теория и практика. 2024. № 10 (238). С. 562-564.
4) Шевко Н.Р., Казанцев С.Я., Хисамутдинова Э.Н. Проблемы противодействия киберпреступности в современных условиях // Криминологический журнал. 2024. № 4. С. 203-207.