Секция «LegalTech. Цифровая криминалистика»

Анализ модели цифрового криминалистического исследования в области промышленного шпионажа (DEIV-IE)

Научный руководитель – Джуманбетова Алтынай Алиевна

Волкова София Сергеевна
Студент (бакалавр)
Московский государственный университет имени М.В.Ломоносова, Юридический факультет, Москва, Россия
E-mail: sophie.volkova16@gmail.com

Исторически сложилось так, что цифровые криминалистические исследования были сосредоточены на быстром получении цифровых улик на месте преступления за ограниченное время и техническом анализе цифровых доказательств. В ходе развития цифровой криминалистики были разработаны различные модели цифровых криминалистических исследований, однако немногие из них уделяют достаточное внимание особенностям расследования и криминалистического исследования преступлений, входящих в состав промышленного шпионажа. [5; 147]

Модель DEIV-IE (Digital Forensic Investigation and Verification Model for Industrial Espionage), предложенная американским специалистом в области цифровой криминалисти Джиён Докко [2; 131], несет в себе две ключевые идеи. Во-первых, в рамках данной модели рассматривается эффективность и надлежащие способы проведения криминалистических исследований при расследовании случаев промышленного шпионажа. Во-вторых, выдвигается авторский взгляд на надлежащую процедуру проверки цифровых доказательств.

Модель DEIV-IE предназначена для работы с отдельно взятым компьютером, на котором установлена операционная система Windows и к которому могут подключаться внешние устройства. В рамках данной модели подразумевается, что исследуемые доказательства были изъяты должным образом и в них не вносились изменения с момента изъятия, то есть вопросы изначальной достоверности цифровых доказательств остаются за пределами модели.

Модель DEIV-IE состоит из шести этапов работы с цифровыми доказательствами в виде файлов: исключение из выборки файлов, которые были созданы без участия пользователя [6]; категоризация оставшихся файлов в зависимости от уровня влияния пользователя на их создание; формирование списка подлежащих выявлению обстоятельств преступления [1]; выявление в созданном массиве файлов тех, которые могут быть использованы для доказывания обозначенных обстоятельств преступления; проверка достаточности полученных в результате выполнения предыдущих этапов доказательств; и, наконец, в случае признания полученных доказательств достаточными - их оформление и документирование для дальнейшего процессуального использования. [3]

Эффективность модели DEIV-IE была экспериментально подтверждена путем испытаний данного подхода на «обучающих расследованиях» - наборах фактов и данных, представленных для обучения криминалистов прокуратурой Кореи и обучающей платформой Corpora [2; 142]. По результатам данного эксперимента, применение модели DEIV-IE позволило обнаружить необходимые для раскрытия преступления доказательства во всех рассматриваемых случаях.

Тем не менее, данная модель обладает рядом недостатков, которые необходимо учитывать при ее применении. Автор DEIV-IE выделяет такие слабые места, как направленность на применение исключительно в отношении индивидуальных компьютеров, затруднения при работе с зашифрованными данными, а также принципиальная необходимость того, чтобы искомые доказательства являлись файлом или содержались в файле [4]. Таким образом, в случае, если рассматриваемый массив информации содержит зашифрованные файлы либо злоумышленниками была уничтожена часть файлов, потребуется предварительная работа по подготовке данных к применению к ним модели DEIV-IE - дешифровка или восстановление данных соответственно.

Несмотря на вышеприведенные недостатки, модель DEIV-IE позволяет значительно улучшить и систематизировать процесс расследования случаев промышленного шпионажа. На сегодняшний день не существует иных моделей цифрового криминалистического исследования, которые учитывают специфику данного вида преступлений. Более того, модель DEIV-IE может быть легко расширена и адаптирована в ответ на появление новых методик промышленного шпионажа, а также основанный на данной модели подход может быть применен к криминалистическим исследованиям и в других технических условиях (к примеру, для иных операционных систем). Также, возможна разработка модели DEIV для других преступлений с учетом их специфики тем же путем, как была создана DEIV-IE для случаев промышленного шпионажа.

В дальнейшем, Джиён Докко планируется разработка программного обеспечения, поддерживающего модель DEIV-IE, для автоматизации работы с файлами в рамках деятельности криминалиста, использующего данную модель.

Источники и литература

1) Bruce, C., Santos, R.B. Crime Pattern Definitions for Tactical Analysis (2011)
2) Jieun Dokko, Michael Shin A Digital Forensic Investigation and Verification Model for Industrial Espionage // Digital Forensics and Cyber Crimeю. New Orleans, 2018. С. 128-146
3) Jieun Dokko Overview of the digital forensic investigation and verification model
4) Jieun Dokko A score obtained by DEIV-IE in the verification cases
5) Montasari, R. Review and assessment of the existing digital forensic investigation process models. Int. J. Comput.
6) National Institute of Standards and Technology (NIST) (2002). The National Software Reference Library