Секция «LegalTech. Цифровая криминалистика»

О некоторых аспектах расследования преступлений, связанных с использованием электронной подписи

Научный руководитель – Фоминых Илья Сергеевич

Олинова Анастасия Евгеньевна

Студент (бакалавр)

Национальный исследовательский Томский государственный университет, Юридический институт, Томск, Россия

E-mail: anastasiaolinova@gmail.com

В настоящее время роль информации в жизни общества выходит на первый план. Разработка новых компьютерных технологий обуславливает появление возможности создания документов на новых носителях, что носит название «электронный документ». Для полноценного использования электронных документов требуется придание им юридической силы, что происходит с помощью удостоверения его электронной подписью. В связи с ростом оборота электронных подписей растёт число преступлений, связанных с подделками и кражами электронных подписей. Поэтому важно знать криминалистические аспекты расследования преступлений, связанных с использованием электронных подписей.

В соответствии со ст. 2 ФЗ «Об электронных подписях», электронная подпись - это «информация в электронной форме, присоединенная к другой информации в электронной форме или иным образом связанная с такой информацией и используемая для определения лица, подписывающего информацию» [2]. Электронная подпись является средством идентификации подписавшего и выражения его согласия.

Ст. 5 ФЗ «Об электронной подписи» [2] устанавливает виды электронной подписи, которые отличаются по уровню надежности и сложности получения: простая электронная подпись и усиленная электронная подпись. Усиленная электронная подпись различается на неквалифицированную и квалифицированную. Таким образом, виды различаются по степени защиты, что имеет значение для данной в плане зависимости аспекта и вида подписи. Если, например, усиленную квалифицированную подпись невозможно взломать, то простую вполне возможно, а это влияет на действия следователя-криминалиста или эксперта при раскрытии преступления, связанного с электронной подписью.

Если говорить о подделке электронной подписи, то она практически невозможна в течение обозримого будущего. В настоящее время есть риски, которые обусловлены неточностью системы идентификации владельца такой подписи, уязвимостями используемого программного обеспечения, а также недоработанностью способа защиты подписи от взлома и похищений. Электронную подпись возможно украсть или получить за другого человека, что связано с человеческим фактором: несоблюдением владельцами правил безопасности в отношении хранения электронной подписи.

Большая проблема состоит в том, как доказать факт использования электронной подписи не владельцем, что является первым аспектом рассматриваемого вопроса. Второй аспект - определение способа, с помощью которого была украдена или взломана электронная подпись. Третьим аспектом является тактика допроса потерпевшего.

Для того, чтобы доказать, что именно владелец данной электронной подписи использовал ее или этой подписью воспользовалось другое лицо, применяется экспертиза электронной подписи, которая относится к категории компьютерно-технических экспертиз [4]. Экспертиза электронной подписи проводится как в судебном, так и во внесудебном и частном

порядке. Производство экспертизы требует специальных познаний в области криптографической защиты данных, которые установлены в ГОСТ Р 34.10-2012 [3]. Перед экспертом ставятся вопросы о принадлежности электронной подписи владельцу, о действительности сертификата, о виде внесения изменений в документ после выставления подписи, о виде электронной подписи и т. п..

Чтобы установить, как она подпись была взломана необходимо знать способы взлома. Электронная подпись состоит из закрытого и открытого ключа. Закрытый ключ известен только владельцу, открытый ключ несёт функцию проверки авторства любым лицом: которому он известен. В работе Гольдвассера, Микали и Ривеста [5] описываются алгоритмы взлома электронной подписи, которые актуальны в настоящее время. К ним относятся: 1. Попытка взлома при использовании только открытого ключа; 2. Взлом при помощи ключей, которые известны злоумышленнику, но которые он не выбирает сам. т .е. он всего лишь обладает перечнем подписей. 3. Взлом при помощи ключей, которые злоумышленник выбирает сам. Результатом этих действий может быть либо полный взлом электронной подписи т. е. получение закрытого ключа, либо подделка такой подписи.

Третьим аспектом является тактика допроса потерпевшего. Потерпевшим является физическое лицо, которому преступлением причинен физический, имущественный, “моральный вред” [1]. В большинстве случаев лицо, похитившее электронную подпись, может быть выявлено через окружение потерпевшего. Грамотно выстроенная тактика, а именно этап постановки вопросов, является одним из самых главных источников информации в данном преступлении.

План допроса должен включать в себя: личные сведения о потерпевшем; место хранения подписи до совершения преступления; знакомы ли потерпевшему лица, которые были осведомлены о наличии у него электронной подписи, и какой информацией об этих лицах он обладает; и т.п.. Помимо выделенных вопросов с учетом обстоятельств дела перечень может дополняться либо сужаться.

Также стоит отметить, что допрос потерпевшего носит, как правило, безконфликтный характер т.е. потерпевший не препятствует установлению истины по делу и поэтому задача следователя при таком допросе заключается в помощи потерпевшему в восстановлении памяти событий, которые могут иметь значение для расследования.

В связи с этим, к тактическим приемам, которые следователи используют при допросе такого потерпевшего можно отнести: во-первых, повторное воспроизведение показаний, во-вторых, детализация некоторых отдельных показаний, в-третьих, оказание помощи потерпевшему в восстановлении в памяти некоторых событий имеющих значение для раскрытия преступления.

Источники и литература

1) Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 30.01.2020) // Собрание законодательства РФ. - 24.12.2001. - N 52 (ч. I). – С. 4921

2) Федеральный закон Российской Федерации от 06.04.2011 г. N 63-ФЗ (ред. от 23.06.2016) "Об электронной подписи" //"Российская газета" – 2011 8 апреля. № 5451

3) ГОСТ Р 34.10-2012. Процессы формирования и проверки электронной цифровой подписи. Введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 7.08.2012 г. N 215-ст: дата введения – 01.01.2013 – URL: http://docs.cntd.ru/document/gost-r-34-10-2012

4) Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. – М.: Право и закон, 2001. – 416 с.

5) S. Goldwasser, S. Micali, R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 17(2):281—308, Apr. 1988. URL: https://dl.acm.org/citation.cfm?id=45480