К вопросу борьбы с преступлениями в сфере оборота документов, защищенных электронно-цифровыми ключами

В. В. Вехов, к.ю.н.,
доцент Волгоградская академия МВД России

Анализ следственной и судебной практики показывает, что за последние 10 лет преступления в сфере оборота конфиденциальных электронных документов, защищенных электронно-цифровыми ключами, получают все большее распространение. Они отличаются высокой общественной опасностью, нанося существенный материальный и моральный ущерб как отдельным потерпевшим – физическим и юридическим лицам, так и в целом авторитету Российской Федерации на международной арене.

Массовый характер приобрели незаконные использования программ для ЭВМ, баз данных, литературных, аудиовизуальных и других произведений, находящихся в электронно-цифровой форме на машинных носителях, а также в памяти ЭВМ и других компьютерных устройств. Например, по данным Главного информационно-аналитического центра при МВД России, за период с 1 января 2001 года по 1 января 2005 года их количество увеличилось в 3,3 раза (для преступлений, уголовная ответственность за которые предусмотрена ст. 146 и 272 УК РФ). При этом, начиная с 1 января 2003 года, их ежегодный прирост составляет 2,1 раза; средний размер причиненного материального ущерба от одного преступления – 559,4 тыс. руб.; 94 % преступлений были совершены в крупном (свыше 50 тыс. руб.) и особо крупном размерах (250 тыс. руб.); в суд с обвинительным заключением направляется только 50,1 % уголовных дел.

Вышеуказанные негативные обстоятельства потребовали координации усилий Федеральных министерств и ведомств по противодействию рассматриваемым преступным посягательствам. Так, 19 апреля 2003 года в свет выходит совместный приказ Министерства экономического развития и МВД России № 132/261 «Об объявлении решения совместного заседания коллегий Минэкономразвития России и МВД России «О мерах по реализации Минэкономразвития России и МВД России государственной политики по защите прав интеллектуальной собственности, пресечению производства и распространения фальсифицированной и контрафактной продукции», в котором, в частности, указаны следующие положения.

1. Уровень поддельной продукции в программном обеспечении и распространении оптических носителей (DVD-дисков) достигает 90 % оборота.

2. В настоящее время имеют место недостаточная техническая оснащенность экспертно-криминалистических подразделений, технических центров, лабораторий, аккредитованных в установленном порядке, и отсутствие современных гармонизированных методик по проведению исследований контрафактной про-

дукции, распространяемой на машинных носителях.

3. Отсутствует единый подход к правовой оценке деяний, связанных с нарушением авторских прав, со стороны правоохранительных органов в субъектах Российской Федерации. Имеющиеся пробелы в законодательстве Российской Федерации создают существенные проблемы при рассмотрении уголовных дел судами общей юрисдикции, что дает возможность организаторам преступлений избегать наказания.

Приказом был утвержден Порядок взаимодействия Министерства экономического развития и торговли Российской Федерации, Министерства внутренних дел Российской Федерации, а также их территориальных управлений и структурных подразделений в сфере охраны объектов интеллектуальной собственности, пресечения производства и распространения фальсифицированной и контрафактной продукции.

Обратим внимание, что в соответствии с п. 3 ст. 48 Закона РФ от 09.07.93 № 5351-I «Об авторском праве и смежных правах» контрафактными являются экземпляры произведения и фонограммы, изготовление или распространение которых влечет за собой нарушение авторских и смежных прав. Согласно ст. 4 этого Закона запись любого авторского произведения в память ЭВМ является его воспроизведением. Причем, как указано в статье 6, авторское право распространяется на произведения, существующие в какой-либо объективной форме, в том числе звуко- или видеозаписи (магнитной, цифровой, оптической и т. д.).

Закон РФ от 29.12.94 № 77-ФЗ «Об обязательном экземпляре документов» определяет *электронные издания* как программы для электронных вычислительных машин и базы данных, а также электронные документы, прошедшие редакционно-издательскую обработку, имеющие выходные сведения, тиражируемые и распространяемые на машинных носителях (п. 1 ст. 5). В свою очередь, *электронный документ* – это документ, в котором информация представлена в электронно-цифровой форме (ст. 3 Закона РФ от 10.01.02 № 1-ФЗ «Об электронной цифровой подписи»).

С 7 января 2002 года введен в действие Межгосударственный стандарт ГОСТ 7.82-2001 «СИБИД. Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления», который устанавливает единые требования к формату и реквизитам электронного ресурса – электронного издания (книги, сборника, статьи, программы для ЭВМ, базы данных, сайта сети Интернет и др., являющихся объектами авторского права).

На основании Закона РФ от 23.09.92 № 3523-I «О правовой охране программ для электронных вычислительных машин и баз данных», программа для ЭВМ и база данных являются объектами авторского права: программа для ЭВМ охраняется как произведение литературы, а база данных – как сборник (п. 2 ст. 2). Правовая охрана распространяется на все виды программ для ЭВМ, в том числе на операционные системы и программные комплексы (п. 3 ст. 3), за исключением идей и принципов организации интерфейса, алгоритма, а также языков программирования (п. 5 ст. 3).

Авторское право на программы для ЭВМ и базы данных не связано с правом собственности на их материальный носитель. Любая передача прав на материальный носитель не влечет за собой передачи каких-либо прав на программы для ЭВМ и базы данных (п. 6 ст. 3).

Только автору программы для ЭВМ или базы данных или иному правообладателю принадлежит исключительное право осуществлять и (или) разрешать осуществление следующих действий (ст. 9 и 10):

- защиту как самой программы для ЭВМ или базы данных, так и их названий от всякого рода искажений или иных посягательств, способных нанести ущерб чести и достоинству автора;
- воспроизведение программы для ЭВМ или базы данных (полное или частичное) в любой форме, любыми способами;
- распространение программы для ЭВМ или базы данных;
- модификацию программы для ЭВМ или базы данных, в том числе перевод программы для ЭВМ или базы данных с одного языка на другой.

Закон РФ от 20.02.95 № 24-ФЗ «Об информации, информатизации и защите информации» определяет *документированную информацию (документ)* как зафиксированную на материальном носителе информацию с реквизитами, позволяющими ее идентифицировать, *конфиденциальную информацию* как документированную информацию, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (ст. 2), и устанавливает правовую защиту на любую документированную информацию, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу (п. 1 ст. 21). Собственник конфиденциального документа имеет право устанавливать в пределах своей компетенции режим и правила его обработки, защиты и доступа к нему (п. 7 ст. 6). В этих целях могут использоваться специальные программно-технические средства защиты (п. 3 ст. 21).

На основании п. 7 Приложения 1 к Положению о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (система сертификации СЗИ-ГТ), утвержденному приказом ФСБ России от 13.11.99 № 564 «Об утверждении положений о системе сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, и о ее знаках соответствия», к ним относятся:

- средства защиты информации от несанкционированного копирования, в том числе средства защиты носителей данных и предотвращения копирования программного обеспечения, установленного на ПЭВМ;
- средства криптографической и стеганографической защиты информации (включая средства маскирова-

ния информации) при ее хранении на носителях данных и при передаче по каналам связи;

- средства прерывания работы программы пользователя при нарушении им правил доступа, в том числе принудительное завершение работы программы и блокировка компьютера;
- средства стирания данных, в том числе стирание остаточной информации, возникающей в процессе обработки секретных данных в оперативной памяти и на магнитных носителях, а также надежное стирание устаревшей информации с магнитных носителей;
- средства выдачи сигнала тревоги при попытке несанкционированного доступа к информации, в том числе регистрации некорректных обращений пользователей к защищаемой информации и организации контроля за действиями пользователей ПЭВМ;
- средства обнаружения и локализации действия программных и программно-технических закладок.

Порядок оборота этих средств на территории Российской Федерации определяется соответствующими нормативно-правовыми актами, например Указом Президента РФ от 03.04.95 № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», Постановлением Правительства РФ от 26.06.95 № 608 «О сертификации средств защиты информации», Постановлением Правительства РФ от 27.05.02. № 348 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации», Постановлением Правительства РФ от 23.09.02 № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» и другими. Они подлежат обязательной сертификации, которая проводится в рамках систем сертификации средств защиты информации.

Средства защиты информации (СЗИ) – это технические, криптографические, программные и другие средства, предназначенные для защиты охраняемой законом информации, средства, в которых они реализованы, а также средства контроля эффективности защиты такой информации. При этом криптографические (шифровальные) средства должны быть отечественного производства и выполнены на основе криптографических алгоритмов, рекомендованных ФСБ России.

Система сертификации средств защиты информации – это совокупность участников сертификации, осуществляющих ее по установленным правилам. Данные системы создаются Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности, Министерством обороны и Службой внешней разведки Российской Федерации, уполномоченными проводить работы по сертификации средств защиты информации в пределах компетенции, определенной для них законодательными и иными нормативными актами Российской Федерации (они именуются – федеральные органы по сертификации). Так, например, системы сертификации средств криптографической защиты информации, в том числе электронной цифровой подписи и электронного ключа на основе криптоалгоритма, создаются ФСБ России (п. 1 Положения о сертификации средств защиты информации). Данный орган федеральной исполнительной власти также осуществляет государственное регулирование в области разработки, производства, реализации и эксплуатации криптографических средств, а также в области предоставления услуг по шифрованию информации в Российской Федерации (Положение о порядке разработки, производства, реализации и использования средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну: Положение ПКЗ-99).

Для решения этих и ряда других смежных задач в структуре ФСБ России функционирует единственное в стране профильное учебное заведение – Академия криптографии Российской Федерации (п. 6 Указа Президента РФ от 11.08.03 № 960 «Вопросы Федеральной службы безопасности Российской Федерации»).

Сертификация СЗИ осуществляется на основании требований государственных стандартов (Постановление Госстандарта РФ от 10.05.2000 № 26 «Об утверждении Правил по проведению сертификации в Российской Федерации»), нормативных документов, утверждаемых Правительством Российской Федерации и федеральными органами по сертификации в пределах их компетенции. В каждой системе сертификации разрабатываются положение об этой системе сертификации, а также перечень средств защиты информации, подлежащих сертификации, и требования, которым эти средства должны удовлетворять.

Сертификационные испытания СЗИ производят испытательные лаборатории федеральных органов по сертификации, которые несут ответственность за полноту испытаний СЗИ и достоверность полученных результатов (п. 6 Положения о сертификации средств защиты информации).

Изготовление и реализация СЗИ на территории России осуществляется исключительно при наличии сертификата. При этом изготовители (продавцы) должны иметь лицензию на соответствующий вид деятельности, связанный с оборотом СЗИ (п. 7 Положения).

Порядок лицензирования деятельности предприятий, учреждений и организаций независимо от их организационно-правовых форм по проведению работ, связанных с созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите информации определяется Положением о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации. *Лицензия* является официальным документом, который разрешает осуществление на определенных условиях конкретного вида деятельности в течение установленного срока. Она

действительна на всей территории Российской Федерации, а также в учреждениях Российской Федерации, находящихся за границей.

В отличие от электронной цифровой подписи, позволяющей не только защитить электронный документ от подделки, но и установить лицо его создавшего, *электронно-цифровой ключ (ЭЦК)* используется исключительно для защиты электронного документа от неправомерного использования и ознакомления с его содержанием. В соответствии со статьей 48.1. Закона Российской Федерации «Об авторском праве и смежных правах» рассматриваемое программно-техническое устройство контролирует доступ к произведениям или объектам авторских и смежных прав, представленных в форме электронных документов, предотвращает либо ограничивает осуществление действий, которые не разрешены автором, обладателем смежных прав или иным обладателем исключительных прав, в отношении произведений или объектов авторских и смежных прав. Такими действиями являются (ч. 2 ст. 48.1):

- действия, направленные на снятие ограничений использования произведений или объектов смежных прав, установленных путем применения технических средств защиты авторского права и смежных прав;
- изготовление, распространение, сдача в прокат, предоставление во временное безвозмездное пользование, импорт, реклама любого устройства или его компонентов, их использование в целях получения дохода либо оказание услуг в случаях, если в результате таких действий становится невозможным использование технических средств защиты авторского права и смежных прав либо эти технические средства не смогут обеспечить надлежащую защиту указанных прав.

Электронно-цифровой ключ, так же как и обычный, используется в совокупности с запирающим устройством (замком). Роль «замка» выполняет специальная служебная программа для ЭВМ – драйвер ЭЦК. При попытке запуска защищенной программы на исполнение или инсталляции ее на другой машинный носитель, драйвер прерывает исполнение этого процесса, обращается к коммутационному порту ЭВМ, проверяет наличие в нем ЭЦК, сверяет его программный код со своим и в случае совпадения возобновляет прерванный ранее процесс (рис. 1).

На основании их технических характеристик представляется возможным определить ***электронно-цифровой ключ*** *как программируемое электронное техническое устройство, изготовленное на базе интегральной микросхемы, содержащей в своей энергонезависимой памяти уникальный код доступа к охраняемой законом компьютерной информации, и являющееся одним из основных элементов программно-технического средства защиты информации.*

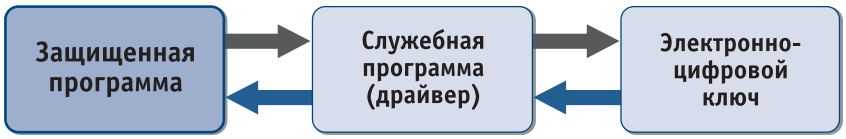

Рис. 1. Принцип работы программы для ЭВМ, защищенной ЭЦК

Таким образом, с программной точки зрения электронно-цифровой ключ – это совокупность знаков, значение которой система использует для определения того, должен ли защищенный ресурс быть доступным процессу, выдавшему данное значение ключа. Указанная совокупность знаков находится в электронно-цифровой форме на материальном носителе, в качестве которого выступает интегральная микросхема – микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функции электронной схемы, элементы и связи которого нераздельно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие (ст. 1 Закона РФ от 23.09.92 г. № 3526-I «О правовой охране топологий интегральных микросхем»). Конструктивно она может быть оформлена в виде:

- обычного USB-накопителя данных (*USB-ключ*, подключаемый к стандартному USB-порту компьютера);
- специального переходного устройства в форме разъемной колодки, подключаемой к стандартному LPT-, COM-порту (*LPT-ключ*);
- металлической таблетки (*ключ iButton*);
- пластиковой карты;
- уникального проводного переходного устройства, подключаемого к клавиатурному порту ПЭВМ и разъему провода клавиатуры (*клавиатурный ключ*).

Анализ следственной практики показывает, что подделка программно-аппаратных средств защиты, функционирующих на основе электронно-цифровых ключей, осуществляется следующими типичными способами, расположенными нами по ранжиру:

- создание и (или) использование программной копии (эмулятора) ЭЦК;
- модификация (переработка) защищенной программы;
- комбинированный способ (комплексное использование способов первой и второй группы).

Создание и (или) использование эмулятора (эмуляция – это имитация функционирования всей или части одной системы средствами другой системы без потери функциональных возможностей или искажения получаемых результатов) – наиболее распространенный способ подделки ЭЦК. Он состоит в написании специальной программы для ЭВМ, которая полностью имитирует работу драйвера защиты и самого ЭЦК. Эмулятор осуществляет программную подмену драйвера ЭЦК, перехватывает обращения защищенной программы к нему и посылает ей правильные ответы по идентификации кода ключа, которого реально нет в порту ПЭВМ (рис. 2). Иными словами, это корректно созданная на программном уровне точная копия ЭЦК и его драйвера, которая вместе с защищенной про-

граммой записывается на один машинный носитель.

Этот способ позволяет преступникам неправомерно использовать защищенную программу, в том числе неограниченное число раз копировать ее вместе с эмулятором на различные машинные носители. Например, 19 июля 2004 года Кировским районным судом города Омска в открытом судебном заседании были рассмотрены материалы уголовного дела в отношении А., обвиняемого в совершении преступлений, предусмотренных ч. 2 ст. 146 и ч. 1 ст. 273 УК РФ. Судом установлено, что А., в период времени с 30 сентября 2002 года по 15 марта 2004 года, находясь при исполнении обязанностей инженера автоматизированных систем управления в ЗАО «Н-Продукт», обладая специальными познаниями в сфере установки и распространения компьютерных программ, имея умысел на причинение ущерба в крупном размере правообладателю бухгалтерской программы ЗАО «1С», умышленно, с целью использования компьютерной программы «УС: Предприятие 7.7 (сетевая версия). Комплексная поставка», незаконно установил ее контрафактные экземпляры на компьютеры нескольких филиалов своего предприятия. Тем самым А. причинил ЗАО «1С» материальный ущерб в крупном размере, исходя из стоимости программного продукта в размере1500 долл. США, что в рублевом эквиваленте на тот период времени составило 217,5 тыс. руб.

Поскольку программа «УС: Предприятие 7.7 (сетевая версия). Комплексная поставка» могла работать в локальной компьютерной сети ЗАО «Н-Продукт» только с уникальным электронно-цифровым ключом HardLock-Server, которого у А. не было, он, с целью обеспечения ее нормальной работы без электронного ключа правообладателя, незаконно установил на компьютеры филиалов ЗАО «Н-Продукт» программу-эмулятор Sable. Эту программу А. скопировал с одного из хакерских интернет-сайтов. По заключению судебной компьютерно-технической экспертизы Sable является вредоносной программой для ЭВМ. На программном уровне она эмулирует (подменяет) работу ЭЦК HardLock-Server, настроенного на защиту компьютерной программы «УС: Предприятие 7.7 (сетевая версия). Комплексная поставка», что позволяет использовать эту программу в нарушении режима охраны, установленного ее правообладателем ЗАО «1С», то есть без подключения соответствующего ЭЦК.

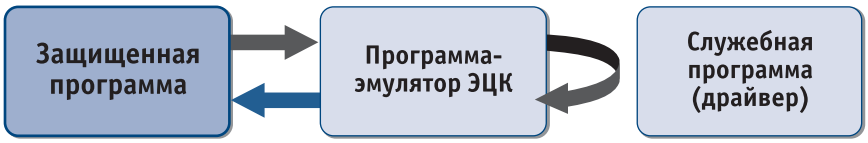

Рис. 2. ***Принцип работы программы – эмулятора ЭЦК***

Суд признал А. виновным в совершении незаконного использования объектов авторского права в крупном размере (ч. 2 ст. 146 УК РФ), а также использовании и распространении программы для ЭВМ, заведомо приводящей к несанкционированному блокированию и модификации информации, нарушению работы ЭВМ, системы ЭВМ и их сети (ч. 1 ст. 273 УК РФ). Ему было назначено наказание в виде одного года и шести месяцев лишения свободы условно с испытательным сроком один год, штрафа в размере 5 тыс. руб. и взыскания в пользу потерпевшего ЗАО «1С» денежной суммы 217,5 тыс. руб. В последующем суд кассационной инстанции признал данный приговор законным, обоснованным и справедливым.

Алгоритм выявления признаков подделки ЭЦК:

- установить наличие работающей защищенной программы;
- установить наличие или отсутствие в порту ЭВМ (системы ЭВМ) ЭЦК;
- попытаться запустить защищенную программу без ЭЦК.

Алгоритм установления местонахождения эмулятора ЭЦК:

- на машинном носителе, на котором находится защищенная программа, произвести поиск программы-эмулятора;
- по всем реквизитам (названию, объему, дате и логическому расположению на носителе) сравнить исполняемые файлы «взломанной» программы с аналогичными файлами защищенной программы – образцом;
- по всем реквизитам сравнить драйвер ЭЦК «взломанной» программы с драйвером-образцом (например, для ЭЦК HASP запустить оригинальный драйвер hinstall-info (образец) и узнать версию драйвера ЭЦК «взломанной» программы; файлы haspnt.sys (для ЭЦК HASP), aksusb.sys, hardlock.sys и hardlock.vxd (для ЭЦК HardLock) пореквизитно сравнить с оригинальными);
- по ключевым словам «emulator», «emu» и другим параметрам произвести поиск папки, в которой может находиться программа-эмулятор;
- путем сканирования реестра операционной системы ЭВМ произвести поиск адресов местонахождения программы-эмулятора.

Модификация является вторым по распространенности в криминальной практике способом подделки ЭЦК. Он заключается в декомпилировании защищенной программы для ЭВМ, определении логики ее подключения к драйверу ЭЦК, отключении связей с ним и компилировании новых логических построений для корректной работы программы. В соответствии со ст. 1 Закона РФ от 23.09.92 № 3523-I «О правовой охране программ для электронных вычислительных машин и баз данных» *декомпилирование программы для ЭВМ* – это технический прием, включающий преобразование объектного кода в исходный текст в целях изучения структуры и кодирования программы для ЭВМ. Этот процесс крайне трудоемкий, поскольку фактически приходится произвести реинжиниринг всей защищенной программы, а в некоторых случаях еще и драйвера ЭЦК. При этом нет гарантии в том, что после выполнения таких операций «взломанная» программа вообще будет работать. ■