О мошенничестве с электронными подписями

Читайте статью «Состав удостоверения документов», в которой основной упор сделан на регламентацию применения и визуализацию электронной подписи, на стр. 34 журнала № 7' 2014

Наталья Храмцовская
к.и.н., ведущий эксперт по управлению документацией компании «ЭОС», эксперт ИСО, член Международного совета архивов

Описаны способы мошеннических действий с электронными подписями на документах – и это не всегда связано со взломом алгоритмов, есть достаточно обходных путей работы с «неопытными» владельцами ключей электронных подписей. Противостоять мошенникам можно, лишь понимая их приемы, на этом мы и сосредоточились в статье. Особо отмечено, что нужно учитывать при долгосрочном архивном хранении электронных документов.
Кроме того, демонстрируются результаты нескольких экспериментов, в которых подписанный документ позже «меняет» отображаемую информацию, а электронная подпись на нем продолжает признаваться достоверной. Это впечатляет!

Читайте статью «Печати и штампы в организации» на стр. 12 журнала № 7' 2014

Технологии достаточно надежные, но…

Технологии электронных подписей и поддерживающая ее технология инфраструктуры открытых ключей имеют репутацию абсолютно надежных. В докладах нередко можно услышать, что их практически невозможно взломать. Но, как показывает практика, нет таких технологий, которые мошенники тем или иным способом не смогли бы обернуть себе на пользу, – и именно на это хотелось бы обратить внимание в первую очередь.

Читайте статью «Факсимиле: определяем правила использования» на стр. 25 журнала № 7' 2014

Это не первая технология, которая объявляется «пуленепробиваемой», и опыт уже показал, что не столько велика угроза возможных злоупотреблений при ее использовании (с которыми можно будет бороться), сколько опасна слепая вера общества и суда в надежность и непогрешимость данной технологии. Как следствие, пострадавшие от нового вида мошенничества люди могут сами быть заподозрены в мошенничестве и привлечены к ответственности.

Читайте ответ на вопрос «Какими ручками и чернилами подписывать документы?» на стр. 86 журнала № 5' 2014

Пример 1

В Великобритании при внедрении высокозащищенных банковских карт нескольких клиентов банков, первыми пострадавших от нового вида мошенничества и обратившихся за компенсацией, сначала отправили в тюрьму по обвинению в вымогательстве и лишь позже разобрались, что кражи совершали сотрудники банка.

Стоит также обратить внимание на то, что некоторые вопросы, связанные с предотвращением мошенничества с использованием электронных подписей, у нас не урегулированы законодательством, хотя уже имеется определенный зарубежный опыт. Негативную роль играет и то, что о проблемах и уязвимостях как-то не принято говорить открыто. Узкий круг специалистов в области информационной безопасности давно об этих проблемах знает, но вот широкие «народные массы» часто не в курсе того, что происходит. А тем временем сфера использования электронных подписей продолжает расширяться…

В мошенничестве с электронными подписями можно выделить 2 разновидности атак:

– *Технические атаки, которые в основном направлены на взлом алгоритмов хеширования*. В настоящее время такой метод мошенничества не слишком опасен, поскольку алгоритмы регулярно обновляются, но вот историкам и тем, кому предстоит обеспечивать долговременное хранение электронных документов, стоит обратить на него самое пристальное внимание. Есть лица, которые заинтересованы в искажении или подделке исторических документов, и для этого им достаточно взломать старые, созданные 20 и более лет назад алгоритмы, а это существенно более простая задача. Документы длительного срока хранения могут иметь значительную ценность, соответственно, последствия мошенничества могут быть серьезными.
– В настоящее время наиболее распространены другие методы мошенничества, связанные *либо с обманом подписывающего документ человека, либо с кражей закрытых ключей*. Кроме того, возрастают риски создания *подставных аккредитованных удостоверяющих центров, способных выпустить квалифицированные сертификаты ключей электронных подписей без ведома людей, указанных в качестве их владельцев.*

Существование и увеличение масштабов мошеннических действий с электронными подписями еще более усложняет проблему архивного хранения таких документов, поскольку архивам в своих стратегиях хранения придется учитывать риски подобного рода.

Доказательство компрометации алгоритма хеширования MD5 (2007-2008 гг.)

Технология электронных цифровых подписей использует метод ассиметричного шифрования, а также метод хеширования, который битовой строке произвольной длины ставит в соответствие битовую строку небольшой фиксированной длины, называемую хешем (дайджестом). Для этого разрабатываются специальные алгоритмы. В частности, алгоритм хеширования проектируется таким образом, чтобы вероятность коллизии – совпадения хешей двух различных строк битов, хотя теоретически

и ненулевая, была бы настолько малой, что за разумное время с использованием самых мощных вычислительных систем сегодняшнего и завтрашнего дня невозможно было бы подобрать другую строку битов, хеш которой совпадает с хешем известной строки битов. На практике это означает невозможность подобрать альтернативное сообщение, на которое можно «перенести» электронную цифровую подпись под известным сообщением так, чтобы она успешно проверялась.

Однако то, что один человек создал, другой всегда сумеет сломать. К настоящему времени ранние алгоритмы ЭЦП уже взломаны. Теоретическая возможность коллизий для алгоритма хеширования MD5, который первоначально широко применялся при создании электронных подписей (и до сих пор все еще используется в ИТ-отрасли для электронного подписания компьютерных программ), была доказана еще в 2004 году группой проф. Ван Сяоюнь (Xiaoyun Wang), однако многие считали эту угрозу не имеющей практического значения.

Китайский математик, профессор Ван Сяоюнь

В 2007 году группа голландских специалистов – Марк Стивенс (Marc Stevens), Арьен Ленстра (Arjen Lenstra) и Бенне де Вегер (Benne de Weger) пообещала предсказать итоги выборов 2008 года в США и сообщила хэш-значение PDF-файла с предсказанием. На самом

Группа голландских специалистов[1]

Слева направо: Бенне де Вегер, Арьен Ленстра, Марк Стивенс, Якоб Аппельбаум, Дэвид Мольнар и Александр Сотиров. Фото: Alexander Klink

[1] http://events.ccc.de/tag/25c3/

деле группа подготовила 12 (!) документов, 10 из которых позже были выложены в Интернете, имевших один и тот же MD5-хэш, – на все возможные (и некоторые невозможные) исходы выборов, см. Пример 2.

Пример 2. Два из подготовленных документов:
первый сообщает о победе на выборах Пэрис Хилтон, второй – о победе Барака Обамы
(у всех документов один и тот же MD5-хэш: 3D515DEAD7AA16560ABA3E9DF05CBC80)

Эта эффектная демонстрация показала, что ЭЦП на основе алгоритма хеширования MD5 могут быть подделаны с использованием вполне доступного оборудования и сравнительно несложных программных инструментов.

Вот и получается, что электронная цифровая подпись, которую мы раньше знали под именем «ЭЦП», а теперь называем «усиленной электронной подписью», не так надежна, как кажется.

С одной стороны, по мере роста мощности компьютеров и развития математики алгоритмы устаревают и все хуже сопротивляются взлому, и очень беспокоит, что большинство коллег пока как следует не осознало последствия того, что электронные цифровые подписи все чаще используются при работе с документами длительного и постоянного срока хранения. У мошенников заинтересованность в подделке таких документов может сохраняться в течение длительного времени. К счастью, пока взлом алгоритмов требует специальных знаний и высокого уровня квалификации, которыми большинство людей не обладает.

При оперативной работе с документами можно не беспокоиться о такого рода уязвимостях, однако потенциальная возможность спустя длительное время изготовить «задним числом» и подложить в архив документы, электронные подписи под которыми будут успешно проверяться, должна тревожить тех, кому приходится работать с электронными документами длительного срока хранения.

С другой стороны, злоумышленники обычно идут по пути наименьшего сопротивления. Существуют другие, более простые и достаточно эффективные приемы, о которых и пойдет речь. Не случайно специалисты часто сравнивают электронную цифровую подпись со стальной сейфовой дверью, установленной в картонном домике. Чем ломать дверь, мошеннику проще или украсть ключи, или уговорить владельца самому ее открыть, или проделать дыру в картонной стене… Некоторые способы вполне по силам даже домохозяйкам.

Некоторые виды мошенничества, не требующие взлома алгоритмов

Наиболее распространенным способом мошенничества с электронными подписями является подписание подписью жертвы подложных документов или транзакций. В настоящее время несанкционированное списание денег через системы «клиент-банк» и интернет-банкинга приняло массовый характер. Как правило, доступ к ключевой информации осуществляется вследствие:

– небрежного отношения к хранению и уничтожению закрытых ключей;
– заражения вредоносными программами устройств, применяемых для подписания документов, а также использования злоумышленниками соответствующим образом «модифицированного» оборудования;
– подписания жертвой специально подготовленных документов, визуальное отображение которых может меняться.

Кроме того, сейчас стала реальностью еще одна угроза, связанная с возможностью создания подставных удостоверяющих центров, имеющих право выпускать усиленные квалифицированные электронные подписи.

Небрежное отношение к хранению и уничтожению закрытых ключей (ключей подписания)

К сожалению, у нас до сих пор среди тех, кто использует электронные цифровые подписи, хватает людей, не понимающих, что электронная подпись – не штампик и не факсимиле.

Пример 3

31.07.2007 приказом Министерства культуры и массовых коммуникаций РФ № 1182 был утвержден «Перечень типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения», который до сих пор действует. Полное непонимание технологии ЭЦП и правовых основ ее применения особенно ярко проявилось в пункте 1954 перечня, в котором для организаций одной из групп был установлен постоянный срок хранения для закрытых ключей ЭЦП.

Правовые последствия применения ЭЦП / усиленной электронной подписи (УЭП) базируются на том, что *закрытый ключ (или, в терминологии закона «Об электронной подписи», ключ подписания) находится под полным контролем владельца ключа.* Он никогда и ни при каких обстоятельствах не передается кому бы то ни было. *Аннулированные закрытые ключи полагается как можно быстрее уничтожать*, чтобы исключить возможность подписания электронных документов задним числом. Более того, для обеспечения максимальной безопасности лучше, чтобы ключевые пары создавались самим владельцем ключа и чтобы закрытый ключ никогда не попадал в чужие руки.

Постоянное хранение закрытого ключа, особенно если к нему есть возможность доступа посторонних лиц, обеспечивает идеальные условия для создания поддельных документов. В то же время закрытый ключ не используется в процессе проверки ЭЦП, поэтому хранить его не требуется.

Читайте новость «Срок хранения отчетов о микрофинансовой деятельности и о персональном составе руководящих органов – 5 лет» на стр. 10 журнала № 7' 2014

Ряд нормативных документов как федерального, так и регионального уровня уже содержит (с некоторыми вариациями) требования об обязательном уничтожении закрытых ключей:

Фрагмент документа

Правила электронного документооборота в системе электронного документооборота Федерального Казначейства (из письма Федерального Казначейства № 42-7.1-17/10.1-102 от 20.03.2007 «О примерном договоре «Об обмене электронными документами»)

4.2.7.12. После окончания срока действия Сертификата его владелец теряет право использования закрытого ключа подписи, соответствующего отзываемому Сертификату, и уничтожает указанный закрытый ключ подписи.

Фрагмент документа

Форма договора об обмене электронными сообщениями при переводе денежных средств в рамках платежной системы Банка России, заключаемого между Банком России и клиентом Банка России (приложение к письму Банка России от 27.03.2013 №51-Т)

6.2. Клиент обязан:
6.2.6. Уничтожать закрытые ключи КА (ЭП) после истечения срока их действия.

С другой стороны, встречаются нормативные акты, согласно которым и уничтожение, и генерация закрытого ключа (ключа подписания) поручается сотрудникам удостоверяющего центра (УЦ) либо оператору информационной системы, что (за исключением случая использования высокозащищенных ключевых носителей, которые обеспечивают создание ключей внутри носителя и не допускают их передачу наружу) является грубейшим нарушением правил информационной безопасности при работе с ключевой информацией:

Фрагмент документа

Регламент удостоверяющего центра Федеральной службы по надзору в сфере образования и науки (утв. распоряжением Рособрнадзора от 18.12.2012 №4436-08)

15.3. Оператор УЦ на основании предоставленного заявления осуществляет уничтожение старой ключевой информации на ключевом контейнере, генерацию ключевых пар, запись закрытого ключа подписи на ключевой носитель, изготовление СКП ЭП (сертификат ключа проверки электронной подписи) и запись СКП ЭП на ключевой носитель.

Фрагмент документа

Регламент регистрации пользователей и поставщиков сведений и подключения их к государственной информационной системе миграционного учета (утв. приказом ФМС РФ № 38, МВД РФ № 91, Минкомсвязи РФ № 32, ФСБ РФ № 76, ФСТЭК РФ № 90 от 19.02.2010)

8. При подключении у пользователя и поставщика сведений АП (абонентских пунктов) или подключении АИС пользователя и поставщика сведений к информационной системе оператор информационной системы обеспечивает:

– изготовление, выдачу уполномоченным лицам пользователя и поставщика сведений, а также уничтожение ключей электронной цифровой подписи...

Если злоумышленник получает в свое распоряжение закрытый ключ, то надежность алгоритмов начинает играть против жертвы. Если электронная подпись успешно проверяется, то очень мало шансов на то, что впоследствии удастся доказать факт подписания документа неуполномоченным лицом и добиться возмещения понесенного ущерба.

Нарушение правил информационной безопасности при подписании электронных документов

Далеко не все понимают: надежность электронных подписей опирается на то, что процесс создания электронной подписи проходит в доверенной среде. Антивирусные компании регулярно оценивают масштабы заражения компьютеров, и на четвертой международной конференции Anti-fraud Russia 2013, прошедшей в ноябре 2013 года, сообщалось, что в России заражена половина компьютеров! Вирусы сейчас все чаще пишутся под конкретное программное обеспечение, используемое для совершения банковских транзакций.

Подписание жертвой специально подготовленных документов, визуальное отображение которых может меняться

В последнее время у нас очень любят дискутировать на тему, что такое электронный документ. Коллеги из ИТ-сферы часто считают электронным

документом любые данные, подписанные электронной подписью. Здесь, однако, есть одна тонкость, хорошо понятная специалистам, занимающимся управлением документами. Важнейшим качеством документа является его неизменность, причем не неизменность его как электронного объекта, а неизменность того, что отображается пользователю. Электронная цифровая подпись позволяет убедиться в неизменности электронного объекта, однако такой объект может представлять собой не только статические данные, но и содержать активный контент (встроенный код, макросы и т.д.), т.е. представлять собой программу, поведение которой может меняться. Достаточно в текст документа включить, например, макрос, показывающий при открытии документа текущую дату.

Эксперимент 1. Подписание PDF-файла, содержащего активный контент

Чтобы продемонстрировать риски, связанные с активным контентом, я провела эксперимент, в котором в PDF-файл был добавлен JavaScript-код (см. Рисунок 1), запрограммированный так, чтобы по истечении 10 минут документ стал нечитаемым – вместо текста отображался зеленый фон. После этого документ был подписан ЭЦП, поддерживаемой программой Adobe Acrobat.

Спустя минуту после подписания файл был снова открыт и была проведена успешная проверка подписи (см. Рисунок 2).

При попытке открыть файл через 11 минут его текст перестал отображаться, но при этом подпись проверяется и подтверждается ее подлинность (хотя Adobe Acrobat все-таки заподозрил, что дело не совсем чисто – он способен это сделать, поскольку «знает» внутреннее устройство документа), см. Рисунок 3.

Рисунок 1. PDF-документ со встроенным JavaScript-кодом

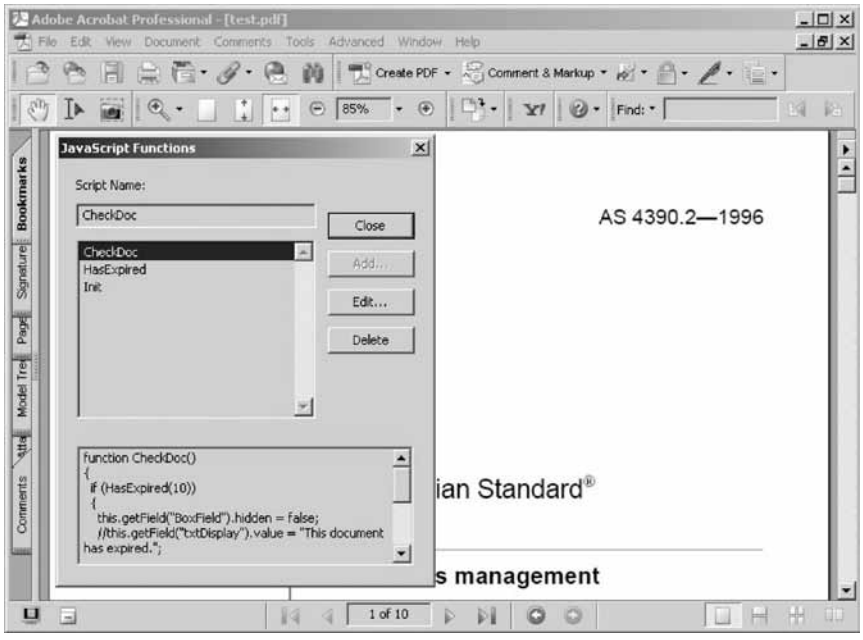


Рисунок 2. Проверка подписи спустя минуту –
все хорошо, документ читается и подпись проверяется

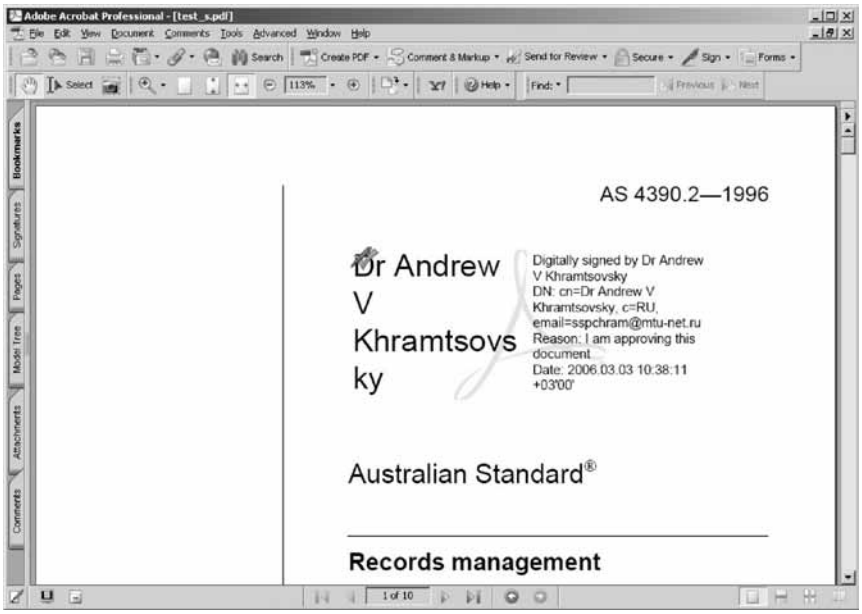
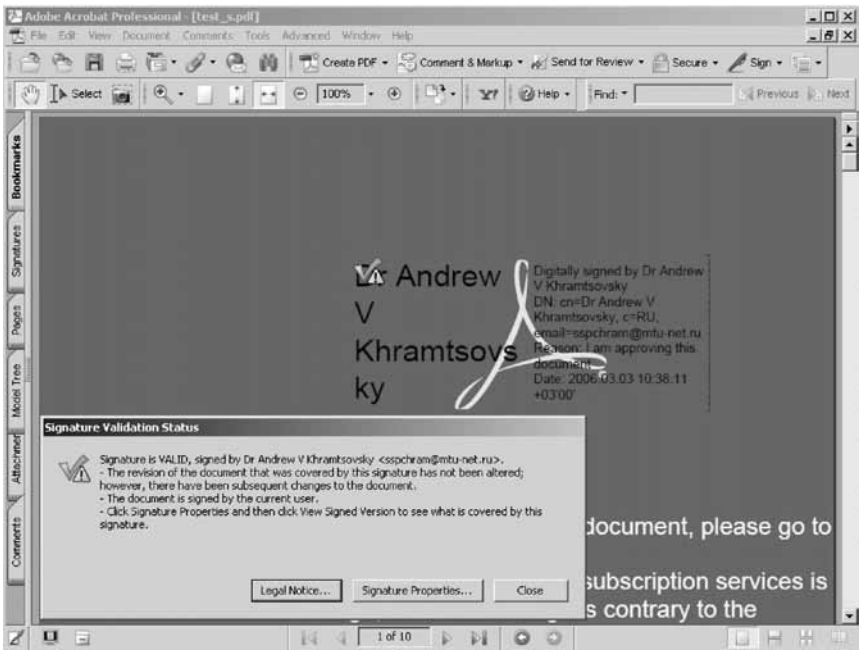


Рисунок 3. Проверка подписи спустя 11 минут –
текст не читается, но подпись проверяется



Недобросовестный контрагент вполне может прислать на подписание PDF-документ, который сегодня показывает один текст, а завтра – другой.

Зарубежный опыт минимизации рисков использования активного контента в электронных документах, подписанных ЭЦП / УЭП

В ряде стран для минимизации подобных рисков приняты меры на законодательном уровне. Так, устанавливается, что выявление встроенного кода в электронном документе приводит к возложению на того, кто его «подсунул» на подписание, обязанности доказывания его безвредности. Наличие активного контента рассматривается как достаточное основание для того, чтобы отказать в принятии документа в качестве доказательства. В нашем законодательстве подобных положений пока не содержится.

В законодательстве *Австрии* установлен явный запрет на использование активного контента:

Фрагмент документа

Указ Федерального канцлера Австрии об электронных подписях 2000 г. (в редакции 2004 г., параграф 4 п. 1) детализирует положения австрийского Закона об электронных подписях

Подписываться электронной подписью могут документы только в тех форматах, что рекомендованы поставщиком сертификационных услуг. Описания таких форматов должны быть общедоступны. Структура формата должна гарантировать неизменный вид документа как во время подписания, так и во время проверки подписи. Если формат допускает кодирование динамических изменений, то не разрешается использовать его элементы, вызывающие динамические изменения.

Согласно нормативной базе *Италии* выявление макросов или исполняемых кодов в электронных документах, подписанных квалифицированными подписями, приводит к тому, что такой документ теряет презумпцию подлинности и его подлинность приходится доказывать:

Фрагмент документа

Декрет Совета министров Италии от 13.01.2004 «Технические правила создания, передачи, хранения, воспроизведения, репродукции и проверки электронных документов»

Электронные документы, подписанные цифровой подписью или усиленной электронной подписью иного вида, основанной на квалифицированном сертификате и созданной при помощи защищенного устройства для создания подписи, не создают эффекта, указанного в п. 3 ст. 10 [презумпция подлинности] сводного текста [Кодекса ЭП], если они включают макросы или исполняемый код, способные изменить представляемые документами акты, факты и данные.

Фрагмент документа

Декрет Совета министров Италии от 30.03.2009 «Технические правила создания, наложения и проверки электронной цифровой подписи» (пункт 3 статьи 3)

Электронные документы, подписанные цифровой подписью или квалифицированной электронной подписью иного вида, не создают эффекта, предусмотренного п. 2 ст. 21 Кодекса [презумпция подлинности], если они включают макросы или исполняемый код, способные изменить представляемые документом акты, факты и данные.

В *Словакии* требования к файловым форматам документов устанавливают стандарты, выпускаемые Государственной службой безопасности, в которых также затрагивается данный вопрос:

Фрагмент документа

Требования к содержанию и формальные спецификации форматов документов, подписываемых усиленной электронной подписью, версия 1, Государственная служба безопасности (NBU) Словакии, 2007

При подписании и проверке подписанных усиленной электронной подписью документов необходимо, помимо самого подписания и проверки подписи, обеспечить также однозначную визуализацию подписанных документов.

Документ специфицирует транспортный формат для подписанных документов, роль которого заключается в обеспечении четкой идентификации типа подписанных документов для целей визуализации.

Документы-«перевертыши»

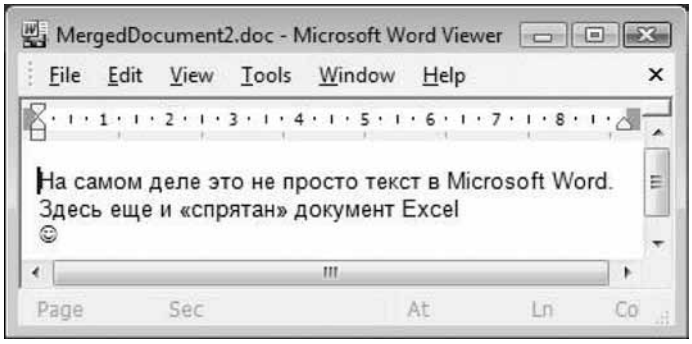
Еще один способ подделки электронного документа связан с использованием технических особенностей форматов. В ряде случаев один и тот же специально подготовленный объект в зависимости от его расширения может отображаться по-разному.

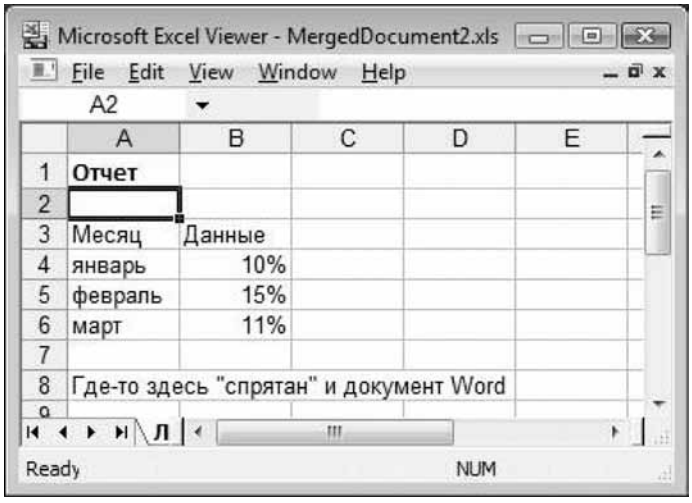
Эксперимент 2. В зависимости от расширения документ отображается по-разному

В 2007 году фирма NT Kernel Resources начала бесплатно распространять программу Merge Streams («Слияние потоков»), позволяющую слить в единое целое документ в формате Word и Excel-таблицу[1]. В зависимости от расширения файла виден или Word-документ, или электронная таблица. Если подписать такой файл ЭЦП / УЭП, то она в обоих случаях будет успешно проверяться.

Это один и тот же файл, однако в зависимости от расширения (.doc или .xls) он отображается по-разному:

[1] Андрей Подкин «Как спрятать документ на видном месте», 15 августа 2007 года, http://ecm-journal.ru/post/Kak-sprjatat-dokument-na-vidnom-meste.aspx.





В 2008 году итальянские специалисты описали аналогичную атаку на статические форматы. Атака строится на создании «полиморфных» файлов, которые показываются по-разному в зависимости от расширения, и на том, что используемые ЭЦП не «покрывают» имя и расширение имени файла.

Франческо Буккафурри (Francesco Buccafurri) в ряде публикаций описал атаку на форматы BMP, TIFF, PDF. Независимо от него сходные результаты опубликовал чешский специалист Петер Рыбар (Peter Rybar).

Итальянское Национальное агентство по вопросам электронного правительства (CNIPA) признало уязвимость очень серьезной и заявило о том, что собирается предусмотреть контрмеры в очередной редакции итальянских правил применения ЭЦП.

Проверка усиленных квалифицированных подписей

При реальном использовании электронной подписи ключевую роль играет вся инфраструктура открытых ключей (PKI) в целом. И здесь наметились проблемы. Если в стране всего несколько аккредитованных удостоверяющих центров, то еще можно поверить в то, что они надле-

жащим образом проверены и сертифицированы. Однако в России аккредитованных удостоверяющих центров стало больше, чем в остальном мире. В «Перечень аккредитованных удостоверяющих центров», размещенный на сайте Минкомсвязи, по данным на 23.03.2014 внесено 338 удостоверяющих центров[2].

Проблема здесь в том, что за вполне умеренные деньги можно создать и аккредитовать удостоверяющий центр, который в нужный момент «вбросит» квалифицированные сертификаты, выданные без ведома лиц, на имя которых они выданы. Согласно закону все квалифицированные сертификаты равноправны, а созданные на их основе подписи приравнены к собственноручным. Жертвам потребуется немало времени и усилий на то, чтобы доказать, что это не их подписи. А тем временем злоумышленники, возможно, уже добьются желаемого результата. Именно ввиду этой угрозы неожиданно *возрос интерес к неквалифицированным подписям, которые используются в рамках договорных отношений и сертификаты ключей которых выдаются одним или несколькими действительно доверенными удостоверяющими центрами.*

Подводя итоги

Учитывая массовость распространения квалифицированных электронных подписей в нашей стране, можно сказать, что именно Россия является сейчас мировым лидером в их использовании, и в ряде случаев нам приходится первыми прокладывать дорогу.

В этих условиях необходимо критически относиться к технологии и понимать, что любой инструмент может быть использован не по назначению – не только во благо, но и во вред.

Важно сформировать разумное отношение к электронным подписям, такое же, как то, что давно сложилось в отношении «живой подписи». Как только люди осознают, что усиленные электронные подписи не являются стопроцентно надежными, они более активно начнут использовать другие технологии, как, например, простую электронную подпись.

Необходимо также внимательно отслеживать правоприменительную практику, выявлять «серые зоны» и оперативно дорабатывать законодательство в области использования электронных подписей.

Технология усиленных электронных подписей / ЭЦП уже продемонстрировала свою полезность и эффективность, но при этом у нее обнаружились и слабые места. С течением времени риск трудно обнаруживаемых атак будет лишь возрастать, поэтому работу с электронными подписями необходимо выстраивать таким образом, чтобы в максимальной степени этот риск снизить.

[2] См.: http://minsvyaz.ru/common/upload/Perechen_A_UZ_ot__22.01.2014.xls