Установление подлинности информации, полученной из недоверенной среды

Финько
Олег Анатольевич,
профессор кафедры обеспечения безопасности информации в автоматизированных системах Военной академии связи (филиал, г. Краснодар), д.т.н., профессор, полковник

Елисеев
Николай Иванович,
доцент кафедры специальной связи Военной академии связи (филиал, г. Краснодар), к.т.н., майор

Развитие информационных вычислительных сетей общего пользования (ИВС ОП) позволило обеспечить массу преимуществ для получения, обработки, хранения и передачи информации. Под ИВС ОП (в соответствии с [1]) понимается всемирная децентрализованно-управляемая совокупность информационных систем, объединенных любыми каналами связи: коммутируемыми или выделенными каналами, локальными или глобальными сетями передачи данных и т. д. Однако для государственных органов и ведомств возможности ИВС ОП крайне ограничены узким перечнем вопросов, решение которых предписано различными законодательными актами (например [2]). При этом значительные возможности ИВС ОП официально остаются невостребованными.

Причиной, ограничивающей возможности ИВС ОП для органов государственной власти, является необходимое условие обеспечения подлинности используемой информации, что зачастую нереализуемо для основной массы информационных ресурсов.

Подлинность информации – комплексное свойство информации соответствовать ряду требований, а именно: целостности, легитимности, достоверности, доступности, а также идентифицируемости автора, места, времени создания информации [3]. В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Статья 2): «*информация – сведения (сообщения, данные) независимо от формы их представления*».

На практике существует два наиболее распространенных пути обеспечения подлинности информации в электронной среде:

1) применение средств электронной подписи (ЭП) или других криптографических средств;
2) обеспечение доверенности среды передачи, хранения, получения и обработки информации за счет использования различных средств разграничения доступа.

Тем не менее следует согласиться и с тем неумолимым фактом, что основным распространенным источником информации в современной практической деятельности должностных лиц часто остаются всевозможные информационные ресурсы, не обеспеченные указанными средствами обеспечения подлинности (средства массовой информации независимо от формы представления информации – бумажной или электронной), ИВС ОП «Интернет» и т.д.). Это в свою очередь снижает достоверность официальных документов, разрабатываемых на основе использования неофициальных ресурсов, несмотря на последующее обеспечение их подлинности легитимными средствами.

Основная причина, по которой основная масса информационных источников остается недоступной для официального использования, – это *отсутствие механизмов доказательства подлинности информации, полученной из данных источников.*

Проблемы обеспечения подлинности информации стандартными средствами ЭП

Наиболее эффективным механизмом, обеспечивающим защиту информации в электронной среде, является ЭП [4]. «Расплатой» за преимущества ЭП является крайне ограниченные возможности ее применения. Эта ограниченность проявляется в том, что в настоящее время ЭП образуется из файла, который помимо информации отражает и формат ее представления. Таким образом, ЭП является функцией, по крайней мере, двух переменных: $f(x_1,x_2)$, где x_1 – информация; x_2 – формат представления информации (сообщения). При этом возникает противоречие между трактовкой определения понятия «информация», даваемого Федеральным законом (№ 149-ФЗ), и существующей практикой обеспечения безопасности информации средствами ЭП.

Под форматом представления информации понимается способ ее наглядного отображения (на экране монитора, бумаге и т.д.). Одна и та же информация может быть представлена как в различных форматах (шрифт, разметка, цвет, элементы мультимедиа и т.д.), так и в различных формах (электронная, бумажная и т.д.). При этом, как правило, каждая система хранения и обработки информации имеет ряд специфических требований к правилам представления одного и того же содержания (например, один и тот же нормативный документ, опубликованный в различных источниках средств массовой информации, может иметь различный формат и бать представлен в различных формах).

Основной формой представления информации в электронной среде является электронное сообщение (ЭС).

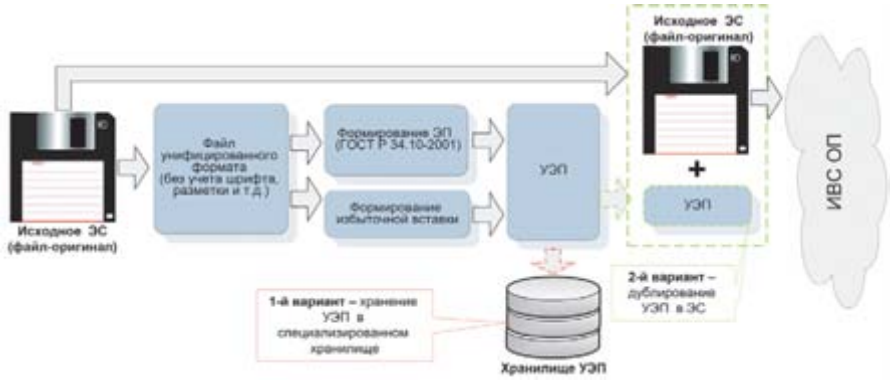

Рис. 1. Пояснение к методу формирования УЭП

Помимо возможного изменения формата представления электронного сообщения в процессе его обработки могут возникать искажения смысловой составляющей. Ярким примером нарушения функционирования механизма ЭП является попытка ее применения для обеспечения целостности копии ЭС, представленной на бумажном носителе. Различные аспекты данной проблемы были неоднократно освещены авторами в рамках докладов на международных конференциях, посвященных информационной безопасности, в частности, на «Инфофорум-2011», «Инфофорум-2012» [5, 6].

Поэтому проблемой применения ЭП для доказательства подлинности информации, полученной из произвольных источников, является необходимость обеспечения нормального функционирования ЭП при исключении из функции переменной x_2 (формат представления сообщения), а также обеспечение устойчивости к погрешностям (в допустимых пределах) в содержимом сообщения x_2.

Метод установления подлинности информации на основе усовершенствованной ЭП

В основе метода установления подлинности информации, полученной из произвольных источников, лежит усовершенствованный метод применения стандартного алгоритма ЭП (ГОСТ Р 34.10-2001), позволяющий обеспечить:

1) инвариантность результата проверки подлинности ЭС к изменениям, не влияющим на смысл сообщения (разметка, шрифт, цвет и т.д.);
2) возможность восстановления целостности сообщения в случае возникновения допустимого количества ошибок текста (нарушения смысла);
3) проверку подлинности ЭС на основе существующего стандарта ГОСТ Р 34.10-2001.

Обозначим элемент, обеспечивающий решение вышеперечисленных задач, как усовершенствованную ЭП (УЭП).

Обеспечение независимости результата проверки подлинности ЭС к искажениям, не влияющим на содержательную часть сообщения, может быть достигнуто путем формирования УЭП от унифицированного формата, инвариантного к изменениям формата текста. Для этого может быть использован, например, язык разметки XML или любой другой формат, отвечающий соответствующим требованиям.

Решением задачи обеспечения целостности содержательной части сообщения (при допустимом количестве непреднамеренных искажений смысловой составляющей) является применение алгоритмов помехоустойчивого многозначного кодирования (например, коды Рида-Соломона, модулярные коды) к элементам ЭС, подлежащим защите (все сообщение или определенные значимые элементы). Избыточное значение может быть внесено в состав сертификата ЭП.

В общем виде метод проверки подлинности информации с использование УЭП включает два основных этапа.

Первый этап. Формирование УЭП:

1) формирование ЭС унифицированного формата (без учета шрифта, разметки, цвета и т.д.);
2) формирование избыточной информации (частный случай построения алгоритма формирования избыточной вставки представлен в [7]);
3) формирование ЭП (в соответствии с ГОСТ Р 34.10-2001) от ЭС унифицированного формата;
4) внесение УЭП, представляющей собой блок избыточной информации и значение ЭП в состав специализированного хранилища (возможно дублирование УЭП в составе ЭС).

Возможность хранения УЭП как в составе ЭС, так и отдельно от него обусловлена логической связью содержания сообщения и элементов УЭП (в отличие от собственноручной подписи, связанной с сообщением физически). Пояснение к методу формирования УЭП представлено на рис. 1. Структура документа с УЭП и его возможная реализация на бумажном носителе представлены на рис. 2 а, б.

Второй этап. Проверка подлинности информации с использованием УЭП:

1) получение информации из ИВС ОП;
2) приведение информации к унифицированному формату ЭС. При необходимости информация должна быть предварительно подвергнута OCR-преобразованию (оцифровке с распознаванием);
3) получение значения УЭП, сформированного от оригинала ЭС (может находиться в составе проверяемого ЭС или быть получено с использованием специализированного хранилища значений УЭП);

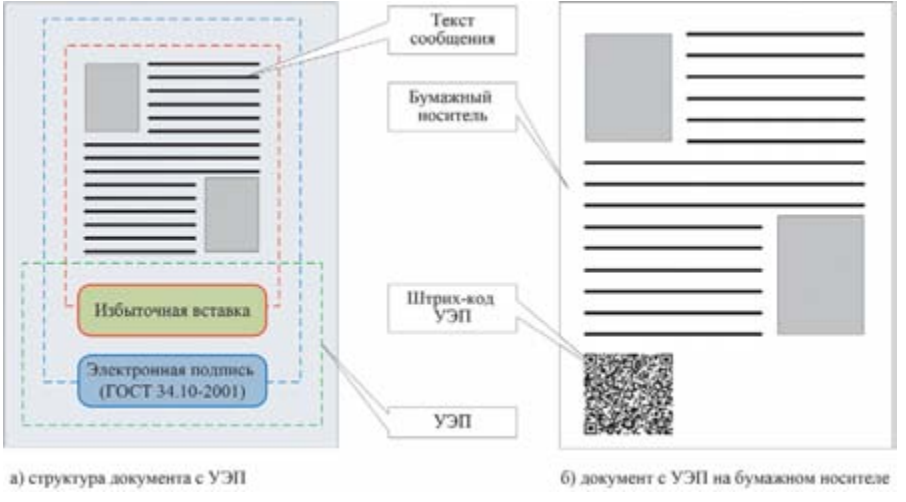

Рис. 2. Общая структура документа с УЭП и его возможная реализация на бумажном носителе

4) вычисление значения ЭП (в соответствии с ГОСТ 34.10-2001) от унифицированного формата проверяемого сообщения;
5) сравнение значения ЭП со значением ЭП из состава УЭП с предшествующим этапом контроля (при необходимости восстановления) целостности ЭС с использованием блока избыточной информации из состава УЭП.

На рис. 3 поясняется процесс подготовки электронного документа к проверке ЭП. Основная задача данной процедуры состоит в подготовке, в общем случае, «нечеткой» по форме представления документа к проверке ЭП, алгоритм которой предполагает оперирование только с четкими образами. Вариант адаптации ЭП для проверки целостности нечетких документов рассматривался авторами в [5]. В целом обобщенный алгоритм проверки подлинности информации с использованием УЭП поясняется с помощью рис. 4.

Рис. 3. Последовательность выполнения этапов подготовки электронного документа к проверке ЭП

Заключение

В статье представлен механизм обеспечения подлинности электронных сообщений, представленных в различных форматах и формах, полученных как из ИВС ОП, так и в результате преобразования сообщений, представленных на бумажных носителях. Последнее позволяет решить проблему включения «бумажных» документов в состав машинных носителей информации и, таким образом, в систему электронного документооборота, сохранив все проверенные практикой преимущества «бумажных» документов для современного и будущего документооборота, исключив конфликт с требованиями ряда руководящих документов.

Ограничением предложенного метода является необходимость введения предварительного этапа формирования УЭП, прежде чем ЭС попадет в ИВС ОП или на бумажный носитель. Однако при положительном решении этого вопроса у пользователя появляются исключительные возможности по установлению подлинности, обеспечиваемой ЭП, для любых сообщений, полученных как из средств массовой информации, так и других информационных источников, не относящихся к доверенной среде необходимого уровня. Хотя процедуру получения подлинной информации всегда можно регламентировать установленным порядком, на практике использование предложенного метода позволит значительно повысить оперативность деятельности правоохранительных и других органов РФ.

Также из-за ограниченности объема статьи за рамки рассмотрения вышли вопросы обеспечения подлинности документов, содержащих графическую информацию.

Рис. 4. Обобщенный алгоритм проверки подлинности информации с использованием УЭП

Литература

1. Директива Начальника Генерального штаба Вооружённых Сил Российской Федерации от 7 июня 1997 г. № 317/2/620 «Об утверждении инструкции по защите информации от несанкционированного доступа при подключении и использовании пользователями Вооруженных Сил Российской Федерации информационных вычислительных сетей общего пользования».
2. Указ Президента Российской Федерации от 17 марта № 351 «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена». – URL: http://www.referent.ru/1/126540 (дата обращения 30.07.2012).
3. Елисеев Н.И., Финько О.А. Системные основы защищенного гибридного документооборота // Тр. междунар. конф. «Управление развитием крупномасштабных систем» / ИПУ РАН. – М., 2011.
4. Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. // Российская газета, № 5451 (75) от 8.04.2011 г.
5. Елисеев Н.И., Финько О.А. Многоуровневая электронная цифровая подпись и алгоритм ее реализации // Инфофорум – 2011: Материалы Юбилейного Национального форума информационной безопасности (Москва, 7-8 февраля 2011 г.). – URL: http://www.infoforum.ru/news/?p=663&n=988 (дата обращения: 30.07.2012).
6. Елисеев Н.И., Финько О.А. Обеспечение подлинности аналоговых документов в системе электронного документооборота МО РФ // Инфофорум – 2012: Материалы Национального форума информационной безопасности (Москва, 7-8 февраля 2012 г.). URL: http://www.2012.infoforum.ru/program (дата обращения: 30.07.2012 г.).
7. Минаков С.В., Финько О.А. Повышение достоверности хранения и передачи первичных текстов на основе гибридной семантико-кодовой избыточности. Известия ЮФУ. Технические науки, 2010. Выпуск журнала, № 4. – URL: http://www.nich.tsure.ru/onti/docs/infbultn/2010_11(112).pdf (дата обращения 30.07.2012).