УДК 004.056

ИССЛЕДОВАНИЕ ВИДОВ ЗАЩИТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Кошеленко Т.А., студентка, кафедра МСТ ХНУРЭ
Вовк А.В., к.т.н., доцент, кафедра МСТ ХНУРЭ

Аннотация. *Проведен анализ различных видов защиты электронных документов. Рассмотрены принципы использования главного реквизита электронного документа, электронной цифровой подписи. Исследованы основные преимущества и недостатки использования тех или иных видов защиты.*

Ключевые слова: *ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ, АУТЕНТИФИКАЦИЯ, ЦИФРОВАЯ ПОДПИСЬ, КРИПТОГРАФИЯ, ЗАЩИТА, ИДЕНТИФИКАЦИЯ.*

Люди всегда уделяли повышенное внимание вопросам защиты и хранения информации, с каждым годом интерес к этой проблеме непрестанно возрастает. Быстрое развитие и становления современных информационно-коммуникационных технологий стало причиной глобальной трансформации индустриального общества в информационное. Все большая часть информации сохраняется и передается в электронном виде.

Благодаря компьютеризации информационной деятельности, общество значительно ускорило процессы поиска, обработки, а также передачи информации. Также существенно повысилась надежность хранения больших массивов информации, что обеспечило дальнейший технический и технологический процесс во всех отраслях. Большинство организаций устанавливают системы электронного документооборота и уже на собственном опыте смогли оценить все преимущества новых технологий работы с документами.

С развитием компьютерных систем возникли новые проблемы, связанные с надежностью и защитой электронных документов. Движение информационных технологий в сторону открытых распределенных систем, широкое распространение сети Интернет как средства межкорпоративного общения придают проблеме информационной защиты особую актуальность. Временами разрушение или утечка информации способны нести куда более значительные финансовые потери, чем затраты на средства защиты.

На данный момент обеспечение защиты электронных документов является очень масштабной и актуальной темой [1, 2], так как практически все сферы базируются на информационных технологиях.

Цель работы – исследовать существующие виды защиты электронных документов для определения их преимуществ и недостатков, а также выбрать наиболее эффективные их них.

На сегодняшний день существует множество способов защиты электронных документов, они имеют большое количество отличий, но их можно разделить на

основные группы: законодательно-правовой, программно-технический и административный.

Рассмотрим используемые сегодня виды защиты электронных документов.

1. Программно-аппаратные комплексы защиты.

Права пользователя на доступ к данным в большинстве компьютерных систем определяется идентифицирующим кодом, по которому система распознает пользователя, и паролем, применяемым для проверки его полномочий.

Обычно пользователь вводит свои реквизиты только в момент регистрации в системе, а пароль является объектом многоразового использования. Так как для профессионала не составит труда определить чужой пароль и идентификатор, этот метод не является самым надежным.

Тем не менее, существует технология, при которой код доступа никогда не повторяется, так как меняется динамически.

Также к программно-аппаратным средствам защиты следует отнести клавиатурный почерк. Распознавание клавиатурного почерка базируется на выборе соответствующего эталона из списка хранимых в памяти компьютера эталонов, на основе оценки степени близости этому эталону параметров почерка одного из операторов, имеющих право на работу с данным компьютером. Решение задачи опознавания пользователя сводится к решению задачи распознавания образов.

Впрочем, при использовании данного способа аутентификации существует сильная зависимость от психофизического состояния оператора.

2. Криптографические методы защиты информации.

Криптография – это наука о защите информации путем ее шифрования от прочтения посторонними. С помощью криптографии представляется возможным преобразование информации таким образом, что ее будет невозможно прочесть без знания ключа.

Свойства, которыми должны обладать методы шифрования:

– законный получатель сможет выполнить обратное преобразование и расшифровать сообщение;

– незаконный получатель, получивший сообщение, не сможет восстановить по нему исходное сообщение без таких затрат времени и средств, которые сделают эту работу нецелесообразной.

Криптосистемы [3] имеют разделение на два класса: симметричные и асимметричные.

В симметричных криптосистемах используют один ключ, как для шифрования, так и для расшифровывания информации.

В то время как асимметричные криптосистемы шифрования имеют разные ключи – закрытый и открытый. Исходный текст шифруется при помощи открытого ключа, который легко вычисляется из закрытого ключа и находится в свободном доступе. В свою очередь, из открытого нельзя вывести закрытый ключ. Для дешифровки используется закрытый ключ, он известен только для получателя сообщения.

Хотя криптографические методы защиты считаются самыми надежными, следует выделить ряд недостатков:

– значительные затраты времени на выполнение преобразований;

– к сохранности ключей предъявляются высокие требования, так как при утере весь документооборот окажется под угрозой;

– проблема распределения ключей.

3. Электронная цифровая подпись.

Электронная цифровая подпись [4, 5] используется для аутентификации информации, с ее помощью можно перенести свойства рукописной подписи под документом в область электронного документооборота. Алгоритм генерации цифровой подписи должен обеспечить невозможность создания правильной подписи без секретного ключа. С помощью открытого ключа можно проверить действительно ли данные были сгенерированы этим секретным ключам.

Обычно цифровые подписи используются для идентификации отправителя, так как предполагается, что только отправитель знает секретный ключ, соответствующий его открытому ключу. Также подписи используют для проставления штампа времени на документах, как подтверждение того, что документ уже существовал в объявленный момент.

Кроме того, цифровые подписи используются для сертификации.

Цифровая подпись документа создается путем генерации дайджеста из документа, к нему добавляется информация о лице, подписывающем документ, штамп времени и прочее. Обычно генерация дайджеста сообщения производится с помощью хэш-функции, которая изменяется при внесении правок в документ. Простейшим дайджестом сообщения можно считать контрольную сумму чисел в двоичном представлении текста сообщения. Получившаяся строка далее зашифровывается секретным ключом подписывающего с использованием того или иного алгоритма. Этот получившийся зашифрованный набор бит и является подписью.

Основные преимущества использования цифровой подписи заключаются в следующем:

– возможность проверки подписи на подлинность;

– поставивший подпись не может от нее оказаться;

– документ, имеющий подпись, не может изменяться;

– возможность подтверждения авторства;

– подпись, поставленная под одним документом, не может быть перенесена в другой.

На практике же полной гарантии выполнения данных свойств дать невозможно, но так как подделывать подписи достаточно сложно, существует большая вероятность уличения мошенников.

4. Организационные мероприятия.

Четкая организация системы документооборота является одной из важнейших мер направленных на защиту информации.

К ряду информационных мероприятий можно отнести:

- обеспечение безопасности рабочих зданий и территории;
- периодический контроль файлов протоколов;
- контроль функционирования систем защиты;
- административное обеспечение;
- контроль доступа на территорию, к определенной информации;
- хранение резервных копий ключевых носителей всех операторов, работающих в системах защиты.

В организационной защите можно регламентировать только приёмы обработки конфиденциальных документов и систему доступа к ним персонала.

Проведя анализ рассмотренных методов можно сделать вывод, что методы и средства защиты информации должны регулярно изменяться с целью предупреждения их раскрытия мошенниками. Используемая система защиты должна быть строго конфиденциальной и специалисты, разработавшие эту систему, никогда не должны быть ее пользователями.

Современные методы защиты постоянно усовершенствуются и повышают надёжность защиты информации, но ни один из них не может дать полной гарантии защиты от мошенничества. С учётом достоинств и недостатков предложенных методов защиты, для обеспечения аутентификации и целостности электронных документов необходимо использовать совокупность различных методов. В то же время в качестве самых надёжных средств защиты можно выделить криптографические методы, при этом установление пароля является одним из простейших средств защиты для пользователя.

Литература.

1. Панасенко, С.П. Защита электронных документов: целостность и конфиденциальность / С.П. Панасенко // Информационные технологии. – 2000. – № 3. – С. 82-87.

2. Киселев, В.Д. Современные проблемы защиты в системах её передачи и обработки / В.Д. Киселев, О.В. Есиков, А.С. Кислицин. − М.: Солид, 2002. – 200 с.

3. Мельников, В.П. Информационная безопасность и защита информации / В.П. Мельников, С.А. Клейменов, А.М. Петраков; под ред. С.А. Клейменова. − 3-е изд., стер. − М.: Изд. Центр «Академия», 2006. − 336 с.

4. Астахова, Л.В. Проблемы организации защищенного документооборота с использованием электронной подписи на предприятиях малого бизнеса / Л.В. Астахова, В.С. Лужнов // Вестник ЮФУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2013. – С. 54-59.

5. Астахова, Т.С. Электронная цифровая подпись как фактор сохранения целостности и аутентичности документа / Т.С. Астахова, Е.П. Чадаева // Известия Томского политехнического университета, Хабаровск.– 2012. – №6. – С. 55-61.

6. Дурняк Б. В. Стандарти в поліграфії та видавничій справі: довідник / Б. В. Дурняк, В. П. Ткаченко, І. Б. Чеботарьова // Львів: Українська академія друкарства, 2011. – 320 с.