СПОСОБЫ ЗАЩИТЫ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ ОТ ФАЛЬСИФИКАЦИИ

Горбачёва Е. Д.
Белорусский государственный университет транспорта
gorbacheva.kate@mail.ru

Прошёл уже достаточно большой промежуток времени с момента изобретения письменности и люди начали использовать более надёжные и подходящие материалы для хранения своей информации. Самым древним способом защиты посланий являлась криптограмма. Информацию шифровали различным способом. Например, меняли местами определённые буквы или заменяли их на цифры или набор символов.

Также были предприняты всякие разные способы для защиты передаваемой информации, секретных сообщений от перехвата. Как вариант, для этого использовали вооружённый конвой.

Сейчас человечество изобрело невероятное множество способов защиты бумажных документов от фальсификации. Некоторые из них перешли в «цифру», а некоторые были придуманы для защиты электронных документов.

Современный уровень развития информационных технологий характеризуется доминированием электронных документов (ЭД) над более привычными для нас бумажными носителями информации. Поэтому главной целью любой организации является защита содержащейся в этих электронных документах информации. [1]

Очень большой угрозе фальсификации подвержены документы носящие бухгалтерское значение. Это могут быть различного рода накладные, бухгалтерские проводки и дт. И чтобы обезопасить такие важные документы от подделки и кражи следует использовать рад определённых

Больше всего в защите от копирования нуждаются рабочие документы электронном расширении. Эти документы в большей степени подвержены краже и фальсификации. Это всё происходит за счёт того, что фирмы, возможно, недостаточно уделяют сил безопасности своих документов, а их кража или фальсификация может стоить организации очень «дорого». Так как сейчас век современных цифровых технологий и мы почти полностью перешли на хранение и обработку информации в электронном виде, то недостаточная защита приведёт к потере очень важной информации или даже так называемый «секрет фирмы» больше не будет являться секретом.

Рассмотрим самые распространённые методы защиты. Как вариант, одним из методов является маркировка. На документе можно указать информационные знаки, позволяющие понять, что его нельзя копировать или редактировать. Самый простой вариант маркировки – это обычная Точка в определённом месте.

Далее, одним из самых распространённых способов защиты электронных документов и ресурсов, является пароль. Пароли можно устанавливать как на

электронный носитель (телефон, ПК и т.д.), так и на сейфы, а также на различные архивы.

Следующий способ – это доступ по цифровому ключу. Данный метод основывается на наличии у пользователя физического ключа (флешки или SD карты) для расшифровки документа. Наличие флешки обеспечивает доступ. То есть файл можно копировать, но скопированный материал нельзя открыть без определенного материального носителя.

Также существуют комбинированные методы защиты документов. Во всех вышеперечисленных методах есть свои достоинства и недостатки. Производители систем защиты документов совершенствуются и постоянно работают над тем, чтобы совместить все сильные стороны в одном решении. Более подходящей кажется такая комбинация:

- Предоставляется доступ к документу по конкретному паролю, который можно отправить по электронной почте или продиктовать по телефону;
- привязка к уникальному материальному носителю, но чтобы не нужно было его дополнительно покупать и доставлять до конечного пользователя;
- возможность управлять правами доступа через интернет, чтобы можно было предоставлять и отзывать доступ к файлу в режиме реального времени;
- отображение на документе специальных меток для обозначения специального режима распространения.

Как пример уникального материального носителя в итоге можно использовать компьютер или мобильное устройство пользователя, например, операционная система и процессор имеют собственные серийные номера, которые нельзя подделать. Это позволит контролировать сколько копий документы было защищено.

Управление правами доступа через интернет обеспечивает DRM. При создании пароля задаются параметры доступа: на каком количестве устройств можно открыть документ, какой промежуток времени будет действовать доступ, есть ли возможность оперативно отозвать доступ. При активации пароля начинают действовать все заданные ограничения.

Метки сами по себе не обеспечивают защиту, но позволяют детектировать утечку по цифровому отпечатку, так как для каждого пользователя подбирается уникальная комбинация цифр и букв, отображаемых на документе.

В настоящее время на рынке существует несколько профессиональных решений, основанных на базе комбинированных методов для защиты электронных документов от копирования и фальсификации. Проведя анализ несколько вариантов, предлагаю познакомиться с сервисами SFContent.com и SFLetter.com.

SFContent.com – профессиональный онлайн-сервис для защиты документов, включающий DRM, привязку к устройству пользователя, использующий водяные метки и серийные номера вместо паролей. Этот сайт предоставляет услуги на платной основе, но есть и бесплатное пробное тестирование. Если доступ к файлам нужно предоставить на период не более 14 дней, то можно воспользоваться пробными серийными номерами, каждый раз открывая новое рабочее пространство в своем аккаунте.

В целом решение достойное и действительно позволяет обеспечить защиту от копирования и редактирования для документов в форматах PDF, DOCX и ряда других.

SFLetter.com. Разработчики данного сервиса позаботились о пользователях чуть больше, чем надо. Они создали не только инструмент для надежной защиты документов от копирования и редактирования, но и полноценную электронную почту, чтобы вы точно были уверены, что ваши данные достигнут получателя в целостности и сохранности. [2]

Помимо этих вариантов можно использовать биометрические данные, как способ защиты электронной информации. Этот вариант хорошо тем, что биометрические данные невозможно подделать. Как, например, отпечаток пальца. Как пример возьмёт телефон, планшет или ПК, хозяин которого использует биометрические данные в качестве защиты своей информации. Сейчас современные технологии позволяют нам защитить как просто устройство от проникновения, так и отдельные файлы или материалы, хранящиеся на данном устройстве. Следовательно, что доступ к этой информации может получить только владелец устройства и никто иной.

Одним из самых эффективных способов защиты бухгалтерских документов может являться электронная подпись. Электронная подпись является реквизитом электронного документа, которая предназначена для защиты данного документа от подделки, полученная в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи, позволяющей произвести идентификацию владельца сертификата ключа подписи, а также избавить владельца и пользователей от искажения информации в электронном документе.

Электронная подпись равнозначна ручной подписи в документе на бумажном носителе при соблюдении определённых условий:

- сертификат ключа должен быть действительным на момент проверки подлинности документа
- цифровая подпись в электронном документе должна быть подтверждена и является подлинной
- данная электронная подпись используется в соответствии с информацией, указанной в сертификате ключа. [3]

Исходя из свей вышеперечисленной информации можно сделать вывод о том, что в настоящее время существуют различные способы защиты бухгалтерских документов от кражи и фальсификации. Многие крупные фирмы уже давно перешли на ведение электронных документов и для их защиты используют некоторые способы, приведённых выше. На мой взгляд, самым доступным и эффективным способом защиты бухгалтерских документов от фальсификации и кражи является электронная подпись, а также использование биометрических данных.

Список использованных источников:

1. Защита электронных документов [Электронный ресурс] – Режим доступа: https://scienceforum.ru, свободный. 27.02.2020.

2. Методы защиты электронных документов от копирования и редактирования [Электронный ресурс] – Режим доступа: https://club.cnews.ru, свободный. 24.02.2020.
3. Электронная подпись [Электронный ресурс] – Режим доступа: https://moluch.ru/archive, свободный. 27.02.2020.