ЭЛЕКТРОННАЯ ПОДПИСЬ КАК СРЕДСТВО ЗАЩИТЫ ИНФОРМАЦИИ ДОКУМЕНТОВ

Куропятникова Алёна Юрьевна

студент, Северо-Кавказский федеральный университет, РФ, г. Ставрополь

Адеева Элина Равилевна

студент, Северо-Кавказский федеральный университет, РФ, г. Ставрополь

В настоящее время широко развиваются и распространяются электронные документы, они применяются не только наряду с бумажными документами, но и вместо них. Сейчас существует большое количество систем электронного документооборота, которые позволяют получить оперативный доступ к любому документу, повышают исполнительскую дисциплину сотрудников, а также безопасно хранят любую информацию, защищая ее от любых попыток несанкционированного использования. Такой документооборот выгоден с точки зрения доступа, перемещения и хранения документов. Электронные документы легко объединяются и формируют базы данных и знаний. Электронные библиотеки уже давно стали удобным способом получения любой информации.

От правильного обращения с электронной документацией зависит успех бизнеса или даже целого предприятия. Информационные технологии помогают применить различные формы организации работы, включая работу вне офиса с помощью электронных платформ хранения информации, электронной бухгалтерии, а также систем поддержки принятия решений.

Сегодня электронный документооборот совершил значительный скачок в своем развитии: электронные услуги все больше набирают популярность и становятся удобными для всех. Ведь в XXI веке, чтобы получить услугу достаточно иметь гаджет и немного времени.

Одним из удобных методов эксплуатации электронных документов является электронная цифровая подпись (ЭЦП) – своего рода собственноручная подпись, настроенная на защиту документа от подделки, полученной в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца подписи (сертификата ключа), а также исключить искажение информации в электронном документе [1]. Федеральный закон №63-ФЗ «Об электронной подписи» от 06.04.2011 г. определяет её как совокупность цифровой информации, присоединённой к электронному документу и подтверждающей его подлинность [2].

Электронная подпись делится на три вида: простая, усиленная неквалифицированная и усиленная квалифицированная.

1. Простая электронная подпись (ПЭП) – наименее надежный вариант подписи, означающий, что электронное сообщение или документ отправлен определенным лицом. ПЭП не может быть использована для подписания документов, содержащих государственную тайну. Данную подпись используют большинство людей для трансакций, связанных с авторизацией по логину и паролю.
2. Усиленная неквалифицированная электронная подпись (НЭП) – подпись, созданная на основе метода криптографического преобразования информации с использованием ключа электронной подписи. НЭП демонстрирует о неизменности документа после его подписания, а в случае видоизменений информации они отобразятся в электронной подписи.

3. Усиленная квалифицированная электронная подпись (КЭП) отличается от других тем, что сертификат ключа данной подписи выдается только аккредитованным удостоверяющим центром или его доверенным лицом. Такая подпись должна быть подтверждена в соответствии требованиям, установленным Законом об электронной подписи [2].

Электронную цифровую подпись может получить как юридическое, так и физическое лицо, в том числе и индивидуальный предприниматель. В случае получения цифровой подписи для организации, то подпись выдается на имя одного из сотрудников, чаще всего – директору.

Подделать электронную цифровую подпись практически невозможно, так как это требует огромное количество времени и вычислений, которые не могут быть выполнены при современном уровне вычислительной техники за оптимальное время, то есть пока информация, хранящаяся в подписанном документе, сохраняет важность и значимость. Работа с ЭЦП позволяет повысить производительность труда и значительно уменьшить время для согласования и утверждения важных документов, но самой важной функцией электронной подписи является защита информации.

Можно с уверенностью сказать, что цифровая подпись обеспечивает несколько видов защиты информации:

- удостоверяет источник документа;

- защищает документ от изменений;

- устанавливает невозможность отказа от авторства.

При проверке ЭЦП используется открытый ключ, соответствующий использованному при вычислении ЭЦП закрытому ключу. Без обладания закрытым ключом и при использовании стойкого алгоритма цифровую подпись подделать нельзя, но и никакие средства шифрования не могут быть абсолютными. Информация становится достаточно зашифрованной и защищенной только, если затраты на его раскрытие превышают цену информации. Если на сегодняшний день защита достаточна, то это не значит, что она будет достаточна завтра. Продолжительность подбора или взлома ключа определяется производительностью компьютера и длиной ключа.

Таблица 1.

Криптографическая стойкость средств электронной цифровой подписи

Симметрии	**Несимметрии**	**Время (ск**
56	384	1-2 с
128	2304	30 с
1024	10000	10 м
2048	30000	сут
4096	1000000	не вскры

Совершенно очевидно, что электронная цифровая подпись вовсе не совершенна, но с применением дополнительных программных, аппаратных и организационных продуктов можно обеспечить защитой информацию от посторонних людей. И все же ЭЦП имеет широкие перспективы внедрения во все сферах жизни информационного общества, связанной с получением, обработкой и передачей информации.

Список литературы:

1. Хошимова Ч.С. Электронная подпись. Защита информации. // Молодой ученый. 2018. №44.

С. 30-33. URL https://moluch.ru/archive/230/53324/ (Дата обращения 17.01.2020)

2. Федеральный закон №63-ФЗ «Об электронной подписи» от 06.04.2011 г. (Дата обращения 17.01.2020)

3. Федеральный закон «Об электронной цифровой подписи» от 10 января 2002 года № 1-ФЗ. (Дата обращения 17.01.2020)