МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ, ИНФОРМАТИКИ И МЕХАНИКИ

КАФЕДРА МАТЕМАТИЧЕСКИХ МЕТОДОВ ИССЛЕДОВАНИЯ ОПЕРАЦИЙ

РЕФЕРАТ
по учебной дисциплине: информационная безопасность
на тему: «Электронно-цифровые подписи. Угроза подделки ЭП. Алгоритмы атак и их осуществление»

Выполнила студентка 2 курса
очного отделения
факультета ПММ
Мальцева А.Ю.
Преподаватель: Крыжановская Ю. А.

Воронеж

2019

Понятие электронно-цифровой подписи

Электронно-цифровая подпись (ЭЦП) - это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Электронно-цифровая подпись - это программно-криптографическое средство, которое обеспечивает:

- проверку целостности документов;
- конфиденциальность документов;
- установление лица, отправившего документ.

Преимущества использования электронно-цифровой подписи

Использование электронно-цифровой подписи позволяет:

- значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;
- усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;
- гарантировать достоверность документации;
- минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;
- построить корпоративную систему обмена документами.

Виды электронно-цифровой подписи

Существует три вида электронной цифровой подписи:

- простая электронно-цифровая подпись;
- усиленная неквалифицированная электронно-цифровая подпись;
- усиленная квалифицированная электронно-цифровая подпись.

Простая электронно-цифровая подпись

Посредством использования кодов, паролей или иных средств, простая электронно-цифровая подпись подтверждает факт формирования электронной подписи определенным лицом.

Простая электронно-цифровая подпись имеет низкую степень защиты.
Она позволяет лишь определить автора документа.
Простая электронно-цифровая подпись не защищает документ от подделки.

Усиленная неквалифицированная электронно-цифровая подпись

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
2) позволяет определить лицо, подписавшее электронный документ;
3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
4) создается с использованием средств электронной подписи.
Усиленная неквалифицированная электронно-цифровая подпись имеет среднюю степень защиты.
Чтобы использовать неквалифицированную электронную подпись, необходим сертификат ключа ее проверки.

Усиленная квалифицированная электронно-цифровая подпись

Для квалифицированной электронной подписи характерны признаки неквалифицированной электронной подписи.

Усиленная квалифицированная электронно-цифровая подпись соответствует следующим дополнительным признакам подписи:

1) ключ проверки электронной подписи указан в квалифицированном сертификате;
2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям законодательства.

Усиленная квалифицированная электронно-цифровая подпись является наиболее универсальной и стандартизованной подписью с высокой степенью защиты.
Документ, визированный такой подписью, аналогичен бумажному варианту с собственноручной подписью.
Использовать такую подпись можно и без каких-либо дополнительных соглашений и регламентов между участниками электронного документооборота.
Если под документом стоит квалифицированная подпись, можно точно определить, какой именно сотрудник организации ее поставил.
А также установить, изменялся ли документ уже после того, как был подписан.

Применение разных видов подписи

1. Простая электронно-цифровая подпись

Обращение заявителей - юридических лиц за получением государственных и муниципальных услуг осуществляется путем подписания обращения уполномоченным лицом с использованием простой электронной подписи.
Использование простой электронной подписи для получения государственной или муниципальной услуги допускается, если федеральными законами или иными нормативными актами не установлен запрет на обращение за получением государственной или муниципальной услуги в электронной форме, а также не установлено использование в этих целях иного вида электронной подписи

2. Усиленная неквалифицированная электронно-цифровая подпись

Случаи, в которых информация в электронной форме, подписанная неквалифицированной электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью, в Налоговом кодексе не определены.

3. Усиленная квалифицированная электронно-цифровая подпись

Для некоторых видов отчетности использование квалифицированной подписи прямо определено нормативными документами.
Например, такой порядок установлен для:

- годовой бухгалтерской отчетности, которую необходимо сдать в Росстат;
- формы РСВ-1 ПФР;
- отчетности в налоговую инспекцию – декларации.

Варианты мошенничества с электронной подписью

1) *Физические преступления* — для развертывания мошеннической схемы необходим контакт преступника с носителем.

1.1. Кража носителя — схема, когда преступник похищает usb-токен, что позволяет ему свободно использовать чужую электронную подпись.
Нейтрализация: — установка пользовательского пароля — напомним, что носители выпускаются со стандартными заводскими паролями,

которые находятся в свободном доступе в интернете и, соответственно, их важно заменить на числовую комбинацию, известную только владельцу. После 3 попыток злоумышленника подобрать пароль, usb-токен блокируется.

1.2. Добровольная передача своей ЭП другому лицу — уполномоченные лица вместо делегирования прав совершать определенные действия передают подчиненным свою электронную подпись. Мошенническая схема может быть развернута и одномоментно, и отложено.
Одномоментно — злоумышленник может использовать электронную подпись непосредственно во время нахождения у него чужого usb-токена.
Отложено — в случае если закрытый ключ ЭП является извлекаемым, преступник может скопировать его и использовать в дальнейшем, уже после возврата носителя владельцу.
Нейтрализация: — никогда, никому и ни при каких обстоятельствах не передавать свою электронную подпись.

1.3. Наличие на токене не декларированных возможностей («закладок») — получение не сертифицированных ключевых носителей из ненадежных источников чревато наличием в программном обеспечении не заявленных в документации включений.
Нейтрализация: — приобретение сертифицированных ФСТЭК носителей — удостовериться в отсутствии «закладок» можно с помощью просвечивания usb-токена рентгеном, что осуществляется в лабораториях Федеральной службы технического и экспортного контроля. Если в результате исследования не было выявлено «закладок», то ключевой носитель признается безопасным и на него выпускают сертификат ФСТЭК.

2) *Технологичные преступления* — для реализации подобных противоправных схем от мошенников в первую очередь требуются навыки в области IT-технологий и информационной безопасности.

2.1. Внедрение злоумышленника в «машину» владельца электронной подписи — мошенник, получивший доступ к компьютеру или ноутбуку жертвы может похитить ключ, скопировав его, в случае если он извлекаемый, или использовать ЭП без ведома владельца.
Нейтрализация: — выполнение правил информационной гигиены — не переходить по подозрительным ссылкам, не скачивать программы и файлы из ненадежных источников, не пользоваться потенциально зараженными флэш-накопителями, установить на компьютер или ноутбук антивирусную программу и прочее.

2.2. *Компрометация канала связи «токен-машина»* — если злоумышленник проникает в канал передачи данных от usb-токена к компьютеру или ноутбуку, то это грозит, в зависимости от типа ключевого носителя, и компрометацией пароля, и компрометацией ключа. Нейтрализация: — выполнение правил информационной гигиены + ФКН — способ предотвратить реализацию подобной схемы, аналогичен предыдущему. В качестве дополнительного средства обезопасить электронную подпись от компрометации можно упомянуть функциональный ключевой носитель (ФКН). ФКН отличается тем, что разделяет вычисления во время генерации ЭП между пользовательским приложением и токеном таким образом, что данные, которые передаются по каналу связи, не позволят преступнику сделать никаких выводов ни о ключе, ни о пароле.

3) *Социальные преступления* — мошеннические схемы, основанные на личных качествах людей, их способности имитировать других, вводить в заблуждение, подделывать документы.

3.1. Получение электронной подписи другим человеком — преступник может завладеть документами нужного лица и, используя максимально похожего на него соучастника, получить ЭП.
Нейтрализация: — ответственное отношение к документам — необходимо хранить документы в надежных местах, а в случае их кражи незамедлительно сообщать в правоохранительные органы.

3.2. Получение электронной подписи по поддельным документам и доверенности — регламент рынка электронной подписи подразумевает обязательную личную явку при первичном получении ЭП, а при повторном выпуске забрать ее можно, предоставив копии необходимых документов и доверенность. Этим и могут воспользоваться мошенники, подделав бумаги.

3.3. Недобросовестность сотрудников удостоверяющих центров — как и в любой системе, будь то правоохранительная, судебная или любая другая, ее рядовые пользователи зависят от тех, кто наделен полномочиями.
Нейтрализация схем 3.2. и 3.3.: — ответственное выполнение сотрудниками УЦ своих обязанностей — в этих случаях предотвращение возможно только внутри удостоверяющих центров при помощи слаженной работы менеджеров, выпускающих ЭП, служб информационной безопасности, подбора персонала и коллег потенциального злоумышленника, что и происходит на современном рынке ЭП.

ЭП не могут быть получены злоумышленниками путем:

1) ЭП могут скопировать с подписанного электронного документа.
2) Теория заговора удостоверяющих центров, которые используют электронные подписи своих клиентов.
3) Закрытый ключ ЭП могут подобрать с помощью открытого, что позволит мошенникам использовать подпись.

Атаки на ЭЦП

Стойкость большинства схем ЭЦП зависит от стойкости ассиметричных алгоритмов шифрования и хэш-функций.

Существует следующая классификация атак на схемы ЭЦП:

- Атака с известным открытым ключем.
- Атака с известными подписанными сообщениями – противник, кроме открытого ключа имеет и набор подписанных сообщений.
- Простая атака с выбором подписанных сообщений – противник имеет возможность выбирать сообщения, при этом открытый ключ он получает после выбора сообщения.
- Направленная атака с выбором сообщения
- Адаптивная атака с выбором сообщения.

Каждая атака преследует определенную цель, которые можно разделить на несколько классов:

- полное раскрытие. Противник находит секретный ключ пользователя
- универсальная подделка. Противник находит алгоритм, функционально аналогичный алгоритму генерации ЭЦП
- селективная подделка. Подделка подписи под выбранным сообщением.
- экзистенциальная подделка. Подделка подписи хотя бы для одного случайно выбранного сообщения.

На практике применение ЭЦП позволяет выявить или предотвратить следующие действия нарушителя:

- отказ одного из участников авторства документа.
- Модификация принятого электронного документа.
- Подделка документа.
- Навязывание сообщений в процессе передачи – противник перехватывает обмен сообщениями и модифицирует их.
- Имитация передачи сообщения.

Так же существуют нарушения, от которых невозможно оградить систему обмена сообщениями – это повтор передачи сообщения и фальсификация времени отправления сообщения.Противодействие данным нарушениям может основываться на использовании временных вставок и строгом учете входящих сообщений.