УДК 004

МОШЕННИЧЕСТВО С ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Дрекслер Д.И., Линиченко Е.И.

Южно-Российский институт управления– филиала РАНХиГС
e-mail:drekslerd01@mail.ru, katya.linichenko@yandex.ru

Аннотация
В статье анализируются тенденции роста использования электронной подписью, приведена статистика количества её пользователей. Приведены способы мошенничества с электронной подписью, а также изучены мнения экспертов по данной теме исследования. Предложены рекомендации по минимизации рисков мошенничества с электронными подписями. Выделены виды ответственности за незаконное использование цифровых подписей.

Ключевые слова: электронная подпись, мошенничество, электронные транзакции, двухфакторная аутентификация, административная ответственность, уголовная ответственность.

ELECTRONIC SIGNATURE FRAUD

Dreksler D.I., Linichenko E.I.

South Russian Institute of Management – branch of RANEPA
e-mail:drekslerd01@mail.ru, katya.linichenko@yandex.ru

Annotation

The article analyzes the growth trends in the use of electronic signatures, and provides statistics on the number of its users. The methods of fraud with an electronic signature are presented, as well as the opinions of experts on this research topic are studied. Recommendations on minimizing the risks of fraud with electronic signatures are proposed. The types of liability for the illegal use of digital signatures are highlighted.

Keywords: electronic signature, fraud, electronic transactions, two-factor authentication, administrative responsibility, criminal liability.

С увеличением использования информационных технологий и систем электронного документооборота (СЭД) выросла популярность электронных подписей (ЭП). Они представляют собой программно-криптографическое средство, которое предназначено для защиты и конфиденциальности электронных ресурсов. Цифровые подписи основаны на публично-частном ключевом шифровании, где для их создания используется приватный ключ, а для проверки – публичный ключ.

Электронные подписи широко используются в современную цифровую эпоху как удобный, эффективный и безопасный способ подписания документов. Они широко применяются в различных сферах, включая банковское дело, правительственные услуги, юридические документы и другие области, где требуется подтверждение подлинности и целостности электронной информации. Они упрощают процессы, снижают бумажную работу и повышают эффективность и надежность электронных операций.

Наш мир становится цифровым, вместе с этим электронные подписи приобретают популярность как средство аутентификации документов и транзакций. Поэтому возникает

вопрос о регулирование отношений в области применения электронной подписи. Они определяются Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» [1]. Данный Федеральный закон и другие нормативно-правовые акты постоянно совершенствуются и учитывают все изменения, происходящие в данной области.

С ростом зависимости от ЭП для различных документов также увеличился и риск мошенничества. Злоумышленники могут подделывать электронные подписи или использовать украденные учетные данные. Исследование мошенничества с электронными подписями является актуальным в наше время. Изучая данную тему, специалисты могут выявить закономерности, уязвимости и лучшие практики для усиления мер безопасности и защиты отдельных лиц и организаций от потенциального вреда.

Исследователи всё чаще поднимают в своих работах и на конференциях вопросы мошенничества с электронной подписью, анализируют существующие незаконные схемы и разрабатывают способы борьбы с ними. На сегодняшний день данная проблема изучена не полностью и требует большого внимания от грамотных специалистов.

С каждым годом растет число пользователей электронной подписью. Они используют ее не только для отчетностей, где это обязательно, но и в документообороте с партнерами и сотрудниками. Согласно удостоверяющему центру «Контур» [2], который работает с 2003 года, в среднем в месяц выдает более 130 тыс. сертификатов. Представим на рисунке 1 темпы роста пользователей электронной подписью УЦ «Контура».

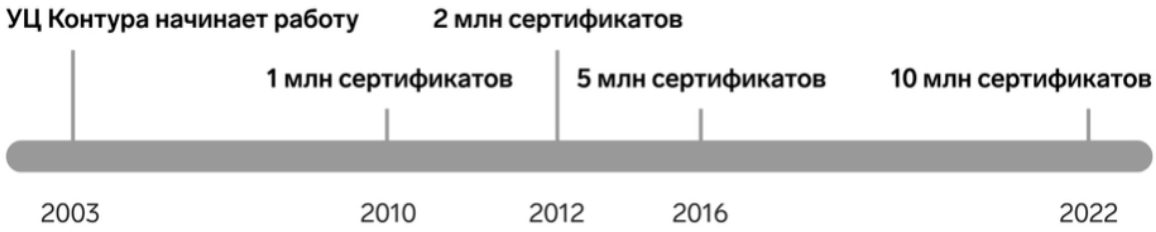

Рис. 1 Количество пользователей электронной подписи УЦ «Контура» [3]

Данная статистика подтверждает, что популярность электронных подписей постоянно увеличивается, но вместе с этим ростом появляются новые способы мошеннических действий. Цифровая подпись обладает большой степенью защищенности в связи с применением стандартов криптографической защиты информации. Однако это не означает, что ЭП полностью защищена.

Существуют несколько способов получения злоумышленниками доступа к электронной подписи:

– украсть ее (физически или виртуально). Злоумышленники могут получить доступ к данным, таким как пароли или идентификационные номера. Это может быть достигнуто путем фишинга, вредоносных программ или взлома баз данных;

– оформить ЭП на кого-то без его ведома;

– использовать чужую ЭП, если введут человека в заблуждение и узнают данные. Мошенники используют манипуляции и обман, чтобы убедить владельца электронной подписи предоставить им доступ или выполнить подпись на поддельном документе.

– купить ЭП, оформленную на подставного человека;

– воспользоваться чужой цифровой подписью, переданной им добровольно. Внутренние работники могут злоупотреблять доступом к электронной подписи, используя его для мошенничества или несанкционированных действий.

– воспользоваться ЭП, выданной сотруднику его бывшим работодателем.

С каждым годом список данных способов пополняется, а методы совершения преступлений подобного рода совершенствуются и становятся наиболее сложными в раскрытие. Поэтому важно детально изучать и разрабатывать методы обеспечения безопасности и подлинности электронных подписей. Организации и учреждения должны активно следить за последними тенденциями и улучшениями в области кибербезопасности.

В исследование TAdviser отмечается, что в России растет уровень мошенничества с поддельными электронными подписями [4]. Директор по методологии и стандартизации Positive Technologies [5] Дмитрий Кузнецов приводит пример того, как сотрудник организации получает доступ к ключу и совершает сделку, на которую не уполномочен, хакеры получают доступ к рабочим местам сотрудников, подписывающих документы, удостоверяющие выдают сертификаты ключевой подписи на основании подложных документов и доверенностей. Это подтверждает проблему роста мошенничества и недостаточной осведомленности руководителей и сотрудников о мерах защиты от несанкционированного использования электронных подписей.

Управляющий RTM Group [6] Евгений Царев отмечает, что известны случаи спорных ситуаций на десятки миллионов рублей, связанные с фальсификацией электронных подписей. Однако подробной статистики об общем ущербе мошеннических действий с ЭП отсутствует, но многие эксперты отмечают, что в некоторых случаях действительно фигурируют большие суммы. Этих сведений достаточно, чтобы утверждать о том, что мошенничество подобного рода является одной из угроз экономической и информационной безопасности.

Совершенствование технических средств, используемыми мошенниками, заставляет задуматься о безопасности ЭП. Необходимо соблюдать определенные рекомендации для того, чтобы защитить электронные подписи от злоумышленников. Важен выбор надежного центра

выдачи электронных подписей. Удостоверяющий центр должен предлагать меры безопасности и соответствовать отраслевым стандартам шифрования и защиты данных. Стоит обращаться за получением ЭП только в аккредитованные удостоверяющие центры. Их список приведен на сайте Министерства цифрового развития, связи и массовых коммуникаций РФ [7].

Необходимо использовать компьютер с достаточной степенью надежности, с высококачественными программами защиты от вирусов. Постоянная поддержка актуальности программного обеспечения электронной подписи и связанных с ним систем с помощью последних обновлений безопасности также является действенным способом защиты. Помимо этого владельцу ЭП стоит всегда помнить о том, что не стоит оставлять свой компьютер в открытом доступе, он также должен быть защищен от физического незаконного воздействия.

Защита ключей электронной подписи имеет решающее значение для обеспечения безопасности и целостности цифровых подписей. Ключ электронной подписи должен оставаться конфиденциальным, чтобы предотвратить несанкционированный доступ и возможное ненадлежащее использование. Необходимо хранить ключ электронной подписи в надежном и зашифрованном месте, устанавливать уникальный пароль для защиты, включая двухфакторную аутентификацию.

Предотвратить возможное злоупотребление электронной подписью может своевременный отзыв сертификата при увольнении сотрудника, которому он был выдан. Аннулирование сертификата ЭП гарантирует, что бывший сотрудник больше не имеет полномочий использовать его для подписания документов, сохраняя безопасность и целостность электронных транзакций. Игнорирование данной процедуры может привести к финансовым расходам.

Подделка и незаконное использование электронной подписи являются серьезными преступлениями, которые могут иметь юридические последствия, которые влекут за собой как и административную, так и уголовную ответственность. В таблице 1 выделим основные статьи и санкции за незаконное использование электронной подписи.

Вид ответственности	**Статья**	**Санкция**
Административная	Ч. 1 ст. 19.23 КоАП РФ	Штраф 30 000-50 000 руб. с конфискацией орудий совершения правонарушения
Административная	Ч. 2 ст. 19.23 КоАП РФ	Штраф 50 000-100 000 руб. с конфискацией орудий совершения правонарушения

Уголовная	Ч. 1 ст. 327 УК РФ	Ограничение свободы на срок до 2 лет, либо принудительные работы на срок до 2 лет, либо арест на срок до 6 месяцев, либо лишение свободы на срок до 2 лет

Табл. 1 Ответственность за подделку и незаконное использование ЭП [8]

Привлечение злоумышленника к ответственности является важным шагом в борьбе со злоупотреблением электронными подписями или их компрометацией. Однако важно помнить, что привлечение к ответственности не обязательно гарантирует возмещение ущерба и убытков. Поэтому необходимо ответственно и сознательно использовать электронную подпись, предпринимая активные действия для предотвращения ее потери или дискредитации.

Таким образом, мошенничество с электронными подписями является важной проблемой в наше время. Такие виды преступлений могут принимать различные формы, включая подделку ЭП, использование украденных подписей, а также манипулирование электронными документами с целью получения поддельного согласия или авторизации.

Необходимо постоянно анализировать новые способы незаконных использований электронных подписей, разрабатывать методы борьбы с ними, совершенствовать меры защиты и информировать население о рекомендациях, которые нужно соблюдать для безопасности электронных подписей. Это может помочь отдельным лицам и организациям защитить себя от рисков, связанных с мошенничеством с электронными подписями.

Литература

1. Федеральный закон «Об электронной подписи» от 06.04.2011г. № 63-ФЗ [Электронный ресурс]. СПС КонсультанПлюс. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_112701/ (дата обращения: 24.10.2023)

2. «КонтурДиадок» [Электронный ресурс]. Официальный сайт. Режим доступа: https://kontur.ru/diadoc (дата обращения: 25.10.2023)

3. Перспективы внедрения электронного документооборота [Электронный ресурс]. Официальный сайт. Режим доступа: https://kontur.ru/diadoc/spravka/38032-perspektivy_vnedreniya_edo (дата обращения: 25.10.2023)

4. В России растет уровень мошенничества с поддельными электронными подписями [Электронный ресурс]. Официальный сайт. Режим доступа: https://tinylinks.ru/mud (дата обращения: 26.10.2023)

5. Positive Technologies [Электронный ресурс]. Официальный сайт. Режим доступа: https://ptsecurity.com/ru-ru/ (дата обращения: 26.10.2023)

6. RTM Group [Электронный ресурс]. Официальный сайт. Режим доступа: https://rtmtech.ru/ (дата обращения: 26.10.2023)

7. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Электронный ресурс]. Официальный сайт. Режим доступа: https://digital.gov.ru/ru/activity/govservices/2/ (дата обращения: 27.10.2023)

8. Подделка электронной подписи: какая ответственность предусмотрена [Электронный ресурс]. Официальный сайт. Режим доступа: https://ppt.ru/art/ecp/poddelka-elektronnoy-podpisi-kakaya-otvetstvennost-predusmotrena (дата обращения: 27.10.2023)