ВЕСТНИК ВОЕННОГО ИННОВАЦИОННОГО ТЕХНОПОЛИСА «ЭРА», 2023, том 4, № 4, с. 372–375

ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

УДК 004.056

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ФУНКЦИОНИРОВАНИЯ ПОДСИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОГО ПРИМЕНЕНИЯ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ ЗА СЧЕТ ВНЕДРЕНИЯ СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

© 2023 г. С. Е. Кияшко[1,*], Д. О. Комиссаров[1], В. А. Волобуев[1], Д. И. Манин[1]

[1]*Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, Краснодар, Россия*

**E-mail: serega-kiyashko1794@yandex.ru*

Поступила в редакцию 08.08.2023 г.
После доработки 09.10.2023 г.
Принята к публикации 09.11.2023 г.

Работа посвящена повышению эффективности функционирования подсистемы обеспечения безопасного применения ключей электронной подписи. Проанализированы нормативно-правовые и руководящие документы в области применения электронной подписи. Рассмотрен алгоритм действия участников электронного взаимодействия в случае нарушения конфиденциальности ключей электронной подписи. Установлено, что владельцы ключевых элементов недостаточно оперативно выявляют факт компрометации. Предлагается автоматизировать данный процесс за счет внедрения системы поддержки принятия решений, построенной на основе методов машинного обучения.

DOI: 10.56304/S2782375X23040083

ВВЕДЕНИЕ

Современные технологии обработки информации предоставляют возможность эффективно управлять различными информационными ресурсами. Одной из востребованных и актуальных задач в этом направлении является внедрение систем электронного документооборота, который позволяет сократить затраты на непроизводительные расходы и оптимизировать трудовой потенциал организаций.

Под электронным документом понимается документ, информация которого представлена в электронной форме [1]. В соответствии с [2] документы независимо от формы или структуры должны обладать следующими свойствами: аутентичностью, достоверностью, целостностью и пригодностью для использования, которые считаются доказательством подлинности деловых событий или операций и полностью отвечают установленным требованиям по ведению деловых операций. Для обеспечения перечисленных выше свойств применяется электронная подпись, под которой понимается информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [3].

ОСНОВНАЯ ЧАСТЬ

Для обеспечения электронного взаимодействия доверенных лиц между собой необходимы как минимум два ключевых компонента: ключ электронной подписи (**КЭП**) и ключ проверки электронной подписи (**КПЭП**). При компрометации первого обеспечить свойства электронных документов невозможно.

Под компрометацией ключа понимается полное или частичное раскрытие информации о секретных или личных криптографических ключах или ключевых материалах, принадлежащих одному или нескольким участникам информационного взаимодействия [4].

На рис. 1 представлен жизненный цикл КЭП при его компрометации.

Удостоверяющий центр по обращению заявителя формирует КЭП и сертификат КПЭП. Метаданные последнего вносятся в реестр сертификатов удостоверяющего центра, где содержится актуальная информация о статусе сертификата и его сроке действия. При наличии действующего сертификата владелец КЭП может подписывать электронные документы, а другие участники электронного взаимодействия проверять подлинность электронной подписи при помощи сертификата КПЭП. В случае нарушения конфиденциальности ключевого элемента его владелец согласно [3] обязан уведомить об этом удостоверяющий центр и

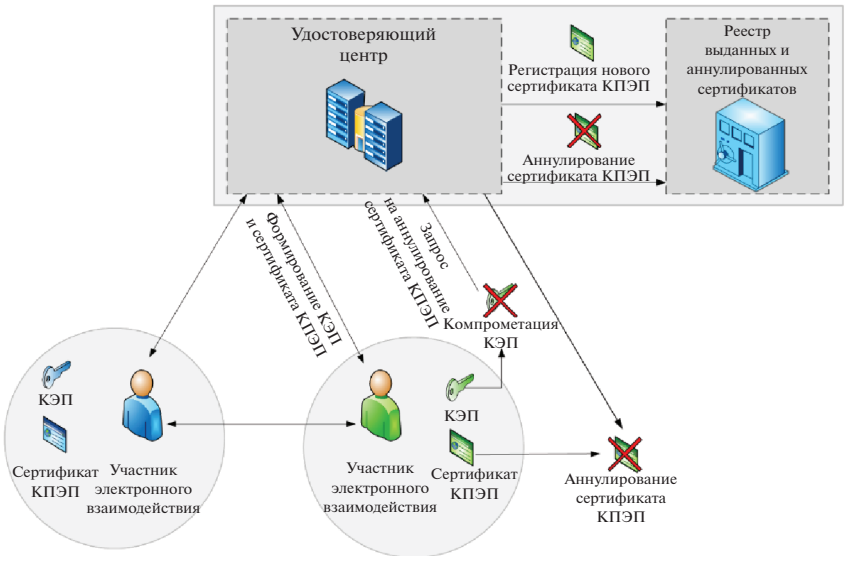

Рис. 1. Жизненный цикл КЭП при его компрометации.

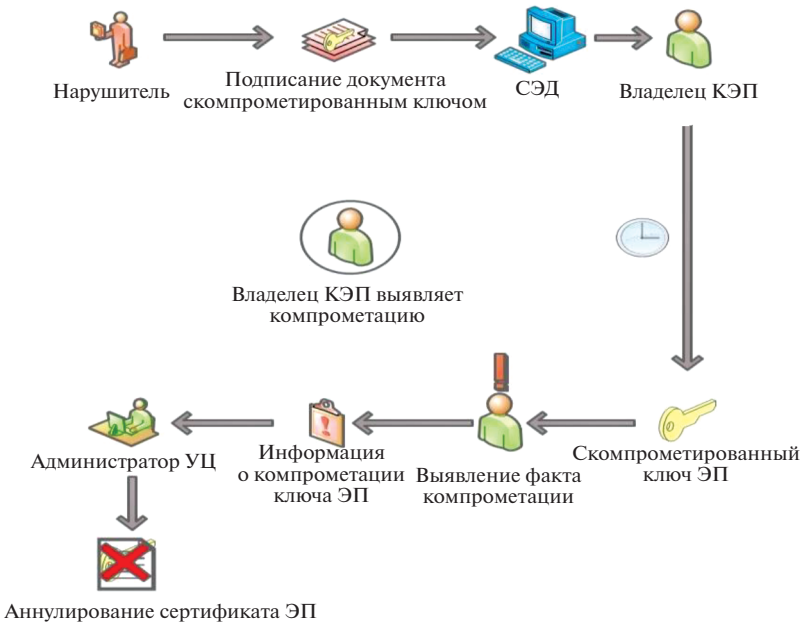

Рис. 2. Подсистема обеспечения безопасного применения КЭП.

иных участников электронного взаимодействия, после чего удостоверяющий центр, выдавший сертификат, аннулирует его и вносит соответствующую информацию в реестр сертификатов.

На рис. 2 детально представлены этап выявления нарушения конфиденциальности КЭП участником электронного взаимодействия и применяемые меры удостоверяющим центром после наступления такого события на примере двух подсистем обеспечения безопасного применения КЭП: существующей и предлагаемой (с использованием системы поддержки принятия решений).

В существующей подсистеме владелец КЭП выявляет факт нарушения конфиденциальности через некоторый промежуток времени t_1 (рис. 3),

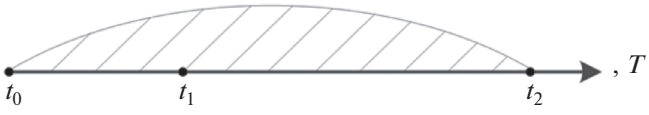

Рис. 3. Срок действия сертификата ключа электронной подписи, где: t_0 – начало действия сертификата КПЭП, t_1 – время обнаружения факта компрометация КЭП, t_2 – конец действия сертификата КПЭП.

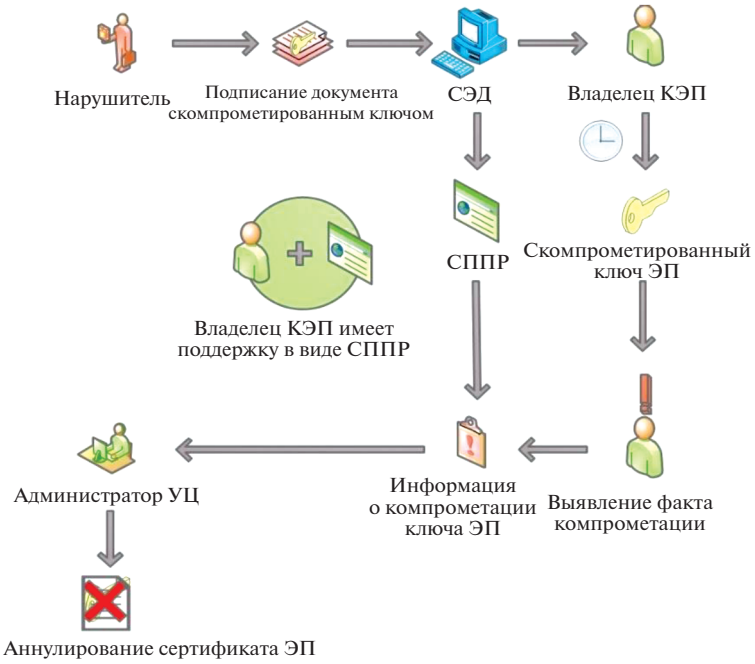

Рис. 4. Подсистема обеспечения безопасного применения КЭП с использованием СППР.

о чем уведомляет удостоверяющий центр, после чего происходит смена ключевых элементов. При редком использовании электронной подписи пользователь может вообще не обнаружить данный факт, тогда $t_1 \to t_2$. И в том и в другом случае несвоевременность обнаружения нарушения конфиденциальности ключа приведет к нанесению характерного ущерба.

Для повышения оперативности выявления фактов компрометации КЭП предлагается внедрить в существующую подсистему обеспечения безопасного применения КЭП систему поддержки принятия решений (**СППР**), реализуемую с использованием методов машинного обучения (рис. 4).

Система поддержки принятия решений в режиме реального времени анализирует метаданные подписанных электронных документов:

– IP-адреса отправителя и получателя;

– день недели и время подписания документов;

– лингвистическое содержание документов.

На основе этих данных СППР в автоматизированном режиме прогнозирует факт нарушения конфиденциальности КЭП и уведомляет об этом администратора удостоверяющего центра для совершения дальнейших действий.

Рассмотрим целевую функцию для определения времени, необходимого для выявления факта компрометации при помощи СППР:

$$T = F(NP_k, N, M, Y) \to \min,$$

где NP_k – сложность k-го алгоритма выявления, N – количество участников электронного взаимодействия, M – метаданные подписанных электронных документов, необходимые для машинного обучения, Y – достоверность прогноза.

При помощи дополнительных ресурсов в качестве СППР время, необходимое для прогнозирования нарушения, стремится к минимальному значению.

ЗАКЛЮЧЕНИЕ

Несвоевременное обнаружение участником электронного взаимодействия факта нарушения конфиденциальности КЭП может привести к получению определенного вида ущерба. Введение СППР минимизирует риски влияния человеческого фактора, выявляя факты компрометации КЭП с высокой оперативностью, повышая эффективность работы подсистемы обеспечения безопасного применения КЭП.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 7.0.8-2013. Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения: национальный стандарт Российской Федерации: дата введения 2014-01-03 / Федеральное агентство по техническому регулированию и метрологии. Изд. официальное. Москва: Стандартинформ, 2014. 6 с.

2. ГОСТ ИСО 15489-1-2019. Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы: национальный стандарт Российской Федерации: дата введения 2020-01-01 / Федеральное агентство по техническому регулированию и метрологии. 12 с.
3. Российская Федерация. Законы. Федеральный закон об электронной подписи: Федеральный закон № 63-ФЗ: [принят Государственной думой 25 марта 2011 года: одобрен Советом Федерации 30 марта 2011 года]. 36 с.
4. Методические рекомендации. Информационная технология. Криптографическая защита информации. Термины и определения. / сост. Сачков В.Н., Черемушкин А.В., Горин А.И. Москва: Технический комитет по стандартизации “Криптографическая защита информации”, 2021 – МР 26.2.006-2021.