Обеспечение гарантий корректности и информационной безопасности(ИБ) ключа ЭП (КЭП) в крупных УЦ

Действительный член Академии криптографии Российской Федерации, **Д. Ф.- М. Н., А.П. БАРАНОВ**

baranov.ap@yandex.ru

К. Т. Н., Ю.А. БАРАНОВ

baranov.ap@yandex.ru

Ключевые проблемы ИБ в крупных УЦ

1. Сохранение конфиденциальности КЭП после его генерации в HSM и создании сертификата ключа проверки ЭП (СКПЭП) в УЦ
2. Физическое соответствие клиента заявляемым данным в СКПЭП
3. Обеспечение ИБ обрабатываемым в УЦ персональным данным (ПД) в географически распределенных УЦ
4. Согласование схемы обработки информации в УЦ по требованиям Регуляторов
5. Пункт 2 не рассматриваем на сегодняшней сессии, поскольку исследовали эту проблему ранее и мало что с тех пор изменилось. Регулятор по этому направлению не определен

baranov.ap@yandex.ru

Основные требования Регуляторов по ИБ, применяемые к УЦ с филиальной сетью

1. Федеральный закон №63-ФЗ об электронной подпис от 06.04.2011
2. Приказ ФСБ России по категорированию ЭП и УЦ (КС1-КА) №796 от 27.12.2011
3. Приказ ФСБ России по доверенным УЦ для УЦ ФНС России №171 от 01.05.2021
4. Приказ ФНС России по УЦ ФНС России и доверенным лицам № ЕД-7-24/340 от25.04.2022
5. Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»
6. Регламенты и приказы с детализацией особенностей ИБ в конкретных УЦ

Действующий порядок работы УЦ по КЭП

1. КЭП порождается в HSM, сертифицированном ФСБ. Заявку на СКПЭП при порожденном Клиентом самостоятельно КЭП здесь не рассматриваем, т.к. это редкий случай
2. Вместе с КЭП вырабатывается КПЭП и КЭП зашифровывается в HSM на пин-коде. Пара шифрованный КЭП и открытый КПЭП направляется оператору УЦ для формированию СКПЭП
3. Аттестованный Токен с шифрованным КЭП и открытым СКПЭП передается Клиенту с запечатанным конвертом, в котором присутствует пин-код
4. Клиент с использованием пин-кода получает доступ к КЭП, а СКПЭП находится в токине в зоне свободного доступа. Далее в зависимости от типа токена КЭП может опять находится в шифрованном с использованием пин-кода Клиента виде
5. Фактически предполагается отсутствие в УЦ внутреннего нарушителя и наличие эффективного контроля за операторами, что в распределенных УЦ реализовывать можно, но сложно

Баланс Требований по участкам и технологиям УЦ

1. Требование 171 Приказа ФСБ России о доверенных УЦ: канал связи Центр-Филиалы защищаются по КБ или КА или фельдъегерской почтой при пересылке КЭП
2. Требование к HSM- уровень – КБ. Цена более 4 млн.Р.
3. Требования к аттестации токена –КС1, что не совсем логично. Тогда уж хотя бы КС3 для ЮЛ, что по крайней мере препятствует действиям группы квалифицированных нападающих не из спецслужб. См. Приказ ФСБ России № 796
4. Поскольку оператор не должен иметь лазейки к содержанию КЭП при проверке корректности СКПЭП, требования к отсутствию НСД и верификации ППО должны быть весьма высокие, которые на Windows сложно выполнимы. Аттестация по Приказу ФСТЭК № 17
5. Оператор должен не иметь возможности отказаться от своих действий. Следовательно, журнал доступа надо шифровать на ключе Администратора или обеспечивать защиту от доступа к нему другими мерами
6. Учитывая высокие цены на шифраппаратуру по уровню КБ для территориально распределенных, с большим числом филиалов УЦ подобное обеспечение накладно, а теперь и затруднительно по времени исполнения больших заказов

baranov.ap@yandex.ru

Безопасность КЭП в обмен на усложнение устройства у Клиента-ЮЛ

1. Правильное требование одноразовой личной идентификации Клиента и заявляемых данных должно непременно сохранятся. Для ЮЛ дополнительный контакт по Интернет не проблема
2. Пользователь инициирует закрытый шифрованный канал на принципе открытого ключа с использованием аттестованного токена или специального ПО
3. В HSM на УЦ вырабатывается КЭП и он зашифровывается на общем с пользователем ключе, причем по уровню КБ пока открытая часть ключа HSM не выходит в систему УЦ
4. КПЭП поступает на обработку в УЦ для формирования СКПЭП и не несет информацию о КЭП
5. Зашифрованный КЭП с открытой частью ключа HSM и открытый СКПЭП направляется по любому каналу Клиенту, где КЭП расшифровывается с помощью токена Клиента или специального ПО, см. п.2

baranov.ap@yandex.ru

Безопасность КЭП для Клиента

1. Безопасность КЭП определяется уровнем безопасности, достигнутом в устройстве Клиента. Возможно до КС3 включительно, а если для связи в УЦ используется КБ, то и до клиентского устройства КБ(что редкость)
2. Безопасность ЮЛ может быть выше чем у ФЛ за счет больших возможностей по сопровождению систем и ответственности
3. Имеющиеся уровень безопасности токенов КС1 трудно признать сейчас достаточным, особенно для предприятий ВПК
4. Клиент должен предварительно или в ходе контакта с УЦ приобрести токен, вырабатывающий ключ для связи с УЦ, и передать свой открытый ключ в УЦ, что при личном посещении не затруднительно ибо токен все равно должен быть у Клиента
5. Связь по Интернету у Клиента ЮЛ имеется, поскольку он сдает отчетность в электронном виде
6. Для сравнения: безопасность иностранной реализации протокола SSL, как и TLS базируется на корневом сертификате неизвестного расположения и надежности

baranov.ap@yandex.ru

Получаемые преимущества по ИБ

1. Блокируется угрозы доступа к КЭП внутреннего нарушителя с квалификацией и возможностями уровня КБ

2. Полезность шифрования КЭП для крупных территориально распределенных УЦ состоит в доступности использования связи между филиалами по КСЗ вместо КБ, при прежнем уровне блокирования угроз

3. Имеется возможность использовать единый для всех филиалов HSM и для рассылки зашифрованного в HSM КЭП использовать любой канал связи, доступный Клиенту

4. Уровень КСЗ достижим для больших территориально распределенных информационных систем при обеспечения требований защиты ПД в УЦ, если ПО в УЦ прошло проверку на отсутствие НДВ, требованиям ФСТЭК и ФСБ России в соответствии с Законом №149

ИБ системы ГОСКЛЮЧ

1. Судя по функциям ГОСКЛЮЧа можно ожидать заявки на доверенное лицо госоргана ФНС при выдаче СКПЭП для ЮЛ(ИП). Письмо ФНС № КВ-4-14/9426@ от 22.07.22
2. Проверка соответствия заявки Клиента и личности заявителя осуществляется на основе считывания телефоном загранпаспорта Клиента, а так же ЕСИА из ПГУ. Физически Клиент не идентифицируется. Нужен только электронный образ паспорта из чипа
3. Данная процедура в принципе в общем виде присутствует в Приказе № 171 п.3, 2021 года, и может быть использована для получения СКПЭП для ЮЛ, если конкретная реализация будет согласована с Регулятором по ИБ
4. Электронный образ паспорта имеется в распоряжении всех отелей и госслужб, где бывал Клиент. Считаных чипов паспортов граждан десятки миллионов.
5. ИБ полученного таким образом КЭП зиждется, по существу, на паре логин-пароль, полученной при регистрации в ПГУ в Почтовом отделении и предъявляемой при каждом обращении за государственной услугой в электронном виде

Спасибо
за внимание

baranov.ap@yandex.ru