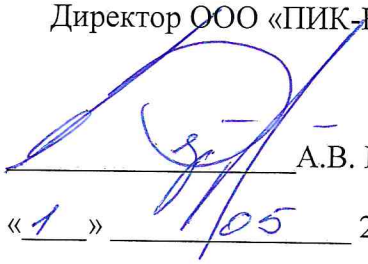
УТВЕРЖДАЮ

Директор ООО «ПИК-Юг»



_____А.В. Берзул

«1» 05 2019 г.

РЕКОМЕНДАЦИИ ВЛАДЕЛЬЦУ ЭЛЕКТРОННОЙ ПОДПИСИ

1. Нормативные документы

Положение разрабатывалось с учетом:

- Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи»;
- Регламента Удостоверяющего центра ООО «НТСсофт»;
- Политика информационной безопасности ООО «ПИК-Юг».

2. Общие положения

2.1. Основные термины:

Электронная подпись (далее ЭП) - 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.

Носитель ключевой информации – носитель информации (смарт-карта, флэш-память, и прочие носители) на которых храниться электронный ключ, предназначенный для защиты электронных взаимодействий.

Сертификат ключа проверки электронной подписи - электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Квалифицированный сертификат ключа проверки электронной подписи (далее - квалифицированный сертификат) - сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным настоящим Федеральным законом и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи (далее - уполномоченный федеральный орган).

Владелец сертификата ключа проверки электронной подписи - лицо, которому в установленном законодательством Российской Федерации порядке выдан сертификат ключа проверки электронной подписи.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи - уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).

Вручение сертификата ключа проверки электронной подписи - передача доверенным лицом удостоверяющего центра изготовленного этим удостоверяющим центром сертификата ключа проверки электронной подписи его владельцу.

Компрометация ключевой информации - утрата, хищение, несанкционированное копирование или подозрение на копирование носителя ключевой информации НКИ или любые другие ситуации, при которых достоверно неизвестно, что произошло с НКИ. **К компрометации ключевой информации также относится увольнение сотрудников, имевших доступ к ключевой информации.**

2.2. Настоящие Рекомендации разработаны для сотрудников и клиентов ООО «ПИК-Юг».

2.3. Данные Рекомендации включают:

— организационные мероприятия по работе с носителем ключевой информации (далее НКИ);

— порядок хранения и использования НКИ;

— порядок действий при компрометации ключевых материалов.

3. Организация работы с носителями ключевой информации

При использовании ЭП владельцы носителей обязаны обеспечивать конфиденциальность ключей ЭП, в частности не допускать использование принадлежащих им ключей ЭП без их согласия.

Владельцы носителей ключевой информации, несут за них персональную ответственность.

4. Хранение и использование ЭП

Пользователю носителей ключевой информации рекомендуется:

— не оставлять носитель ключевой информации в компьютере, после использования НКИ для подписи или шифрования - извлечь носитель;

— не использовать для работы носитель с нарушенной целостностью;

— не оставлять персональный ключевой носитель без личного присмотра, где бы то ни было;

— не передавать свой персональный ключевой носитель другим лицам (за исключением случаев, когда имеются соответствующие документы: акт, доверенность и т.п.);

— не делать неучтенные копии ключевой информации, распечатывать или переписывать с нее файлы на иной носитель информации;

— не использовать персональный ключевой носитель на заведомо неисправном компьютере.

Владелец ЭП обязан обеспечить конфиденциальность ключа, и в частности не разрешать использовать ключ без согласия самого владельца.

В случае если собственником сертификата и ключа является юридическое лицо, и необходимо передать ЭП в пользование сотруднику, оформляется приказ по общей деятельности предприятия.

Если передача производится не сотруднику компании, либо владельцем является физическое лицо – необходимо оформить доверенность.

Следует помнить: при передаче ключа или без него невозможно фактически установить, кто именно подписывает документ с помощью ЭП - владелец, сотрудник или чужой человек. В этом случае пользователь, получающий документы и информацию, не имеет достоверных сведений и надеется на честность и законопослушность владельца.

Все риски и ответственность электронной подписи при ее передаче несет владелец.

5. Порядок действий при компрометации носителей ключевой информации

К событиям, связанным с компрометацией ключевой информации должны быть отнесены следующие события:

— утрата ключевого носителя;

— утрата ключевого носителя с последующим обнаружением;

— увольнение сотрудников, имевших доступ к ключевой информации;

— возникновение подозрений на утечку информации или ее искажения в системе связи.

При компрометации ключей ЭП владельцу следует немедленно:

— прекратить передачу информации с использованием скомпрометированных ключей ЭП или шифрования;

— сообщить о факте компрометации в ООО «ПИК-Юг»;

— подать заявление на аннулирование действия сертификата при наличии оснований полагать, что конфиденциальность ключа нарушена.

ООО «ПИК-Юг» до момента получения такого уведомления не несет ответственности, связанной с возможными неблагоприятными последствиями для Владельца сертификата ключа проверки ЭП.