Удостоверяющий центр ООО «АйтиКом»

Руководство по обеспечению безопасности использования электронной подписи и средств электронной подписи

Материал для владельцев ЭП

1. Общие положения

Настоящее Руководство составлено в соответствии с требованиями Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» и является средством официального информирования лиц, владеющих квалифицированным сертификатом ключа проверки электронной подписи (далее – сертификат), об условиях, рисках и порядке использования усиленной квалифицированной электронной подписи (далее – квалифицированная ЭП) и средств электронной подписи, а также о мерах, необходимых для обеспечения безопасности при использовании квалифицированной ЭП.

Основные риски при использовании электронной подписи (далее – ЭП) связаны с несанкционированным доступом к ключам ЭП (т.е. использованием без ведома их владельца), вследствие чего становится возможным возникновение электронных документов, порождающих нежелательные юридически значимые последствия в отношении владельца сертификата ЭП. Источниками несанкционированного доступа могут быть как преднамеренные либо неумышленные действия человека, так и активность вредоносного программного обеспечения. Далее приводится краткий перечень основных мер безопасности для владельцев ЭП, направленных на избежание указанных рисков.

Определить круг лиц, имеющих доступ с согласия владельца сертификата ЭП к ключам и средствам ЭП, а также обязанности и ответственность этих лиц по обеспечению конфиденциальности ключей ЭП.

Исключить пребывание посторонних лиц в помещениях с ключами и средствами ЭП, их доступ к рабочему месту, либо, в случае необходимости пребывания, обеспечить контроль над их действиями.

Определить порядок обращения с ключевыми носителями при использовании и хранении, исключающий возможность несанкционированного доступа к ним.

Установить и использовать на рабочем месте лицензионное программное обеспечение (далее — ПО) стабильных версий, полученное из вызывающих доверие источников. Не использовать измененные, взломанные или неподдерживаемые производителем версии ПО.

Установить и использовать на рабочих местах антивирусное ПО.

Установить или использовать уже имеющиеся на рабочих местах средства межсетевого экранирования (firewall) с определением правил доступа к сетевым ресурсам. Установить и использовать средства ЭП строго в соответствии с эксплуатационной документацией.

Регулярно отслеживать и устанавливать обновления безопасности для ПО, обновлять антивирусные базы.

Разработать и использовать политику назначения и смены паролей (на вход в операционную систему, параметры BIOS, экранную заставку и т.д.) в соответствии с общепринятыми рекомендациями по созданию сильных паролей. При покидании рабочего места с активным сеансом пользователя блокировать его паролем.

При наличии оснований полагать, что конфиденциальность ключа ЭП нарушена (произошла компрометация ключа), немедленно принять меры по прекращению действия сертификата ЭП.

К событиям, связанным с компрометацией, относятся, включая, но не ограничиваясь, следующие:

• потеря ключевых носителей, в том числе с их последующим обнаружением;

• увольнение сотрудников, имевших доступ к ключевой информации;

• нарушение правил хранения ключевых носителей;

• возникновение подозрений на утечку информации. Не использовать для создания ЭП ключи, если известно, что эти ключи используются или использовались ранее лицами, не имеющими доступа к ним.

2. Требования и рекомендации по обеспечению информационной безопасности на рабочем месте пользователя

2.1 Подключение АРМ к сетям общего пользования

При использовании СКЗИ на АРМ, подключенных к сетям общего пользования, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей. В качестве такой меры рекомендуется установка и использование на АРМ средств межсетевого экранирования. Должен быть закрыт доступ ко всем неиспользуемым сетевым портам.

В случае подключения АРМ с установленным СКЗИ к общедоступным сетям передачи данных необходимо ограничить возможность открытия и исполнения файлов и скриптовых объектов (JavaScript, VBScript, ActiveX и т.д.), полученных из сетей общего пользования, без проведения соответствующих проверок на предмет содержания в них программных закладок и вредоносных программ.

2.2 Обращение с ключевыми носителями

В организации должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации с ключами ЭП и шифрования, который должен исключать возможность несанкционированного доступа к ним.

Для хранения ключевых носителей в помещениях должны устанавливаться надежные металлические хранилища (сейфы), оборудованные надежными запирающими устройствами.

Запрещается:

•Снимать несанкционированные администратором безопасности копии с ключевых носителей;

•Знакомить с содержанием ключевых носителей или передавать ключевые носители лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей (монитор) АРМ или принтер;

- Устанавливать ключевой носитель в считывающее устройство ПЭВМ АРМ в режимах, не предусмотренных функционированием системы, а также устанавливать носитель в другие ПЭВМ;
- Записывать на ключевой носитель постороннюю информацию.

2.3 Обращение с ключевой информацией

Владелец сертификата ключа проверки ЭП обязан:

- Соблюдать конфиденциальность ключа ЭП, т.е. не допускать его использование без согласия;
- Немедленно требовать приостановления действия сертификата ключа проверки ЭП при наличии оснований полагать, что конфиденциальность ключа ЭП (закрытого ключа) нарушена (произошла компрометация ключа);
- Обновлять сертификат ключа проверки ЭП в соответствии с установленным регламентом.