РУКОВОДСТВО

пользователя Удостоверяющего центра Общества с ограниченной ответственностью «Сампо-Сервис» по обеспечению информационной безопасности при использовании средств электронной подписи

Используемые сокращения

ИБ – информационная безопасность
ОС – операционная система
РС – рабочая станция
СКЗИ – средство криптографической защиты информации
СКПЭП – сертификат ключа проверки электронной подписи
УЦ – удостоверяющий центр Общества с ограниченной ответственностью «Сампо-Сервис»
ЭД – электронный документ
ЭП – электронная подпись

Настоящее руководство предназначено для информирования пользователей УЦ о порядке обеспечения информационной безопасности в процессе использования ЭП и средств ЭП, о рисках, связанных с использованием ЭП.

Риски использования ЭП

При использовании ЭП существуют следующие основные риски:

- Риски, связанные с аутентификацией (подтверждением подлинности) пользователя. Лицо, на которого указывает СКПЭП ЭП ЭД, может заявить о том, что ЭП сфальсифицирована и не принадлежит данному лицу.
- Риски, связанные с отказом от содержимого ЭД. Лицо, на которое указывает СКПЭП ЭП ЭД, может заявить о том, что ЭД был изменен и не соответствует ЭД, подписанному данным лицом.
- Риски, связанные с юридической значимостью ЭД. В случае судебного разбирательства одна из сторон может заявить о том, что ЭД с ЭП не может порождать юридически значимых последствий или считаться достаточным доказательством в суде.
- Риски, связанные с несоответствием условий использования ЭП установленному порядку. В случае использования ЭП с нарушением установленного согласно требованиям законодательства или соглашениям между участниками электронного взаимодействия порядка, юридическая сила подписанных в данном случае ЭД может быть поставлена под сомнение.
- Риски, связанные с несанкционированным доступом (использованием ключа ЭП без согласия владельца). В случае компрометации ключа ЭП или несанкционированного доступа к средствам ЭП может быть получен ЭД, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

Для устранения указанных рисков предусмотрен комплекс организационных и технических мер обеспечения ИБ, основанных на соблюдении пользователем требований нормативных актов регуляторов, уполномоченных в сфере защиты информации, и применении сертифицированных в установленном законодательством Российской Федерации порядке средств ЭП в соответствии с требованиями технической и эксплуатационной документации.

Обязанности пользователей УЦ по обеспечению безопасности использования ЭП

Для обеспечения безопасности использования квалифицированной ЭП УЦ обязаны:

- Обеспечить конфиденциальность ключей ЭП.
- Применять для формирования ЭП только действующий ключ ЭП.
- Не применять ключ ЭП при наличии оснований полагать, что данный ключ был скомпрометирован.
- Применять ключ ЭП с учетом ограничений, содержащихся в квалифицированном СКПЭП (расширения Extended Key Usage, Application Policy, Certificate Policies сертификата), если такие ограничения были установлены.
- Немедленно обратиться в УЦ с заявлением об аннулировании (прекращении действия) СКПЭП в случае нарушения (или подозрения в нарушении) конфиденциальности ключа ЭП (компрометация ключа).

- Не использовать ключ ЭП, связанный с квалифицированным СКПЭП, заявление об аннулировании (прекращении действия) которого подано в УЦ, в течение времени, исчисляемого с момента времени подачи заявления в УЦ по момент времени официального уведомления об аннулировании (прекращении действия) сертификата, либо об отказе в аннулировании (прекращении действия).
- Не использовать ключ ЭП, связанный с СКПЭП, который аннулирован или действие которого прекращено.
- Использовать для создания и проверки квалифицированных ЭП, создания ключей ЭП и ключей проверки ЭП сертифицированные в установленном порядке средства ЭП.
- Соблюдать требования «Регламента оказания услуг Удостоверяющего центра Общества с ограниченной ответственностью «Сампо-Сервис».

Рекомендации по обеспечению безопасности автоматизированного рабочего места

- Рекомендуется организовать отдельную РС для эксплуатации СКЗИ и использовать её исключительно в целях взаимодействия с целевыми информационными системами (электронные торговые площадки, gosuslugi и т.п.).
- Необходимо ограничить физический доступ посторонних лиц к РС путем размещения оборудования РС в служебных помещениях, для которых обеспечен режим ограниченного доступа.
- Необходимо использовать исключительно лицензионное программное обеспечение и организовать его регулярное обновление.
- На РС должна быть установлена только одна ОС.
- Не допускается установка на РС средств разработки и отладки программного обеспечения. Если средства отладки приложений необходимы для технологических потребностей пользователя УЦ, то их использование должно быть разрешено администратором безопасности. При этом запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ. Необходимо исключить попадание в систему средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам, а также программ, позволяющих, пользуясь ошибками ОС, получать привилегии администратора.
- Рекомендуется исключить использование режима автоматического входа пользователя в ОС при её загрузке.
- Рекомендуется исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек, системного реестра, для всех, включая группу Administrators.
- Все неиспользуемые ресурсы системы рекомендуется отключить (протоколы, сервисы и т.п.).
- Рекомендуется ограничить возможности пользователя запуском только тех приложений, которые разрешены администратором безопасности.
- Рекомендуется организовать затирание временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это невыполнимо, то ОС должна использоваться в однопользовательском режиме и на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям.
- Должны быть установлены ограничения на доступ пользователей к системному реестру в соответствии с принятой в организации политикой безопасности, что реализуется при помощи ACL или установкой прав доступа при наличие NTFS.
- На все директории, содержащие системные файлы Windows и программы из комплекта СКЗИ, должны быть установлены права доступа, запрещающие запись всем пользователям, кроме Администратора (Administrator), Создателя/Владельца (Creator/Owner) и Системы (System).
- Должна быть исключена возможность создания аварийного дампа оперативной памяти, так как он может содержать криптографически опасную информацию.
- Рекомендуется обеспечить ведение журналов аудита, при этом она должна быть настроена на завершение работы при переполнении журналов.
- Рекомендуется произвести настройку параметров системного реестра в соответствии с эксплуатационной документацией на СКЗИ.
- Установка и настройка СКЗИ должна выполняться в присутствии администратора, ответственного за работоспособность компьютера и только с дистрибутива, полученного по доверенному каналу.

- Установка СКЗИ и первичная инициализация ключевой информации осуществляется в соответствии с эксплуатационной документацией на СКЗИ. При установке СКЗИ должен быть обеспечен контроль целостности и достоверность дистрибутива СКЗИ.
- Перед установкой требуется произвести проверку ОС на отсутствие вредоносных программ с помощью средств антивирусной защиты информации, имеющих актуальные базы сигнатур.
- По завершении инициализации осуществляются настройка и контроль работоспособности программного обеспечения РС.
- В ОС РС для каждого сотрудника, допущенного к работе с СКЗИ, рекомендуется завести уникальную учетную запись с ограниченными правами доступа.
- Стандартные учетные записи User и Administrator ОС РС рекомендуется переименовать, а также установить пароли для данных учетных записей.
- Необходимо отключите в ОС РС гостевую учетную запись (Guest).
- Необходимо установить на РС средство антивирусной защиты и, по возможности, персональный межсетевой экран.
- Необходимо осуществлять регулярное обновление антивирусных баз сигнатур.
- Необходимо регулярно проводить полную антивирусную проверку РС (не реже, чем один раз в неделю).
- Необходимо проверять все съёмные электронные носители, подключаемые к РС (DVD/CD, USB-flash носители и др.), на предмет наличия вирусов и иного вредоносного кода.
- Необходимо использовать надежные пароли - длиной не менее 8 символов, содержащие буквы из различных регистров (заглавные и строчные), специальные символы (*, &, ^, % и т.п.) и цифры. Не используйте очевидные сочетания (имя, фамилия, дата рождения, номер телефона). Пароль доступа к системе должен отличаться от PIN-кода USB-токена.
- Рекомендуется как можно чаще менять пароли доступа в ОС РС (не реже, чем один раз в квартал).
- Необходимо запоминать свой пароль и PIN-код USB-токена, а не записывать его на бумаге, хранить в текстовых файлах и пр. Не допускается сообщать персональный пароль и PIN-код лицам, не допущенным к работе с соответствующими средствами ЭП.
- Не допускается загружать и устанавливать программное обеспечение, полученное из непроверенных источников (электронная почта, Интернет и пр.).
- Сетевое оборудование, обеспечивающее доступ организации в сеть Интернет, должно блокировать любые сетевые пакеты, передаваемые с РС на серверы, не относящиеся к серверам целевых информационных систем, службам обновления установленного системного и прикладного программного обеспечения, антивирусных баз. Доступ ко всем неиспользуемым сетевым портам должен быть закрыт.
- Рекомендуется использовать СКЗИ в однопользовательском режиме.
- Рекомендуется использовать на границе периметра локальной вычислительной сети средства межсетевого экранирования, обнаружения/предотвращения вторжений (IDS/IPS), потокового антивирусного сканирования.
- Не допускается оставлять без контроля при включенном питании и загруженном программном обеспечении СКЗИ после ввода ключевой информации. При уходе владельца квалифицированного СКПЭП со своего рабочего места должно использоваться автоматическое включение экранной заставки, защищенной паролем. В отдельных случаях (при невозможности использования парольной защиты) допускается загрузка ОС без запроса пароля, однако при этом должны быть реализованы дополнительные организационно-технические меры, исключающие несанкционированный доступ.
- Рекомендуется предусмотреть возможность исключить несанкционированное изменения аппаратной части компьютера. Например, опечатыванием системного блока администратором. Также возможно применение специальных сертифицированных средств защиты информации – аппаратно-программных модулей доверенной загрузки (например, «Соболь» или «Аккорд» и т. п.).
- Рекомендуется исключить возможность загрузки и использования ОС, отличной от установленной на РС (например, отключив в BIOS функцию загрузки с CD/DVD приводов, USB-flash дисков и т. п.). Доступ к изменению настроек BIOS РС должен быть защищен надежным паролем. Также для данных целей возможно применение аппаратно-программных модулей доверенной загрузки.
- В случае подключения компьютера 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.

Рекомендации по работе с ключевыми носителями:

- Необходимо обеспечить ограниченный доступ к носителям ключевой информации путем хранения в сейфе (запираемом шкафе и пр.).
- По завершении рабочего дня носитель ключевой информации должен быть помещен в сейф (запираемый металлический шкаф и пр.).
- Использовать носитель ключевой информации рекомендуется исключительно на РС.
- Носители ключевой информации могут быть предоставлены исключительно лицам, допущенным к их использованию.
- Рекомендуется избегать посещения сторонних ресурсов сети Интернет во время работы на РС.
- Запрещается устанавливать ключевой носитель в считывающее устройство в режимах, не предусмотренных функционированием системы.
- Запрещается использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ

Организационные мероприятия по обеспечению ИБ

- Пользователем УЦ должен быть определен и утвержден список лиц, имеющих доступ к ключевым носителям.
- Пользователем УЦ должен быть определен и утвержден порядок учета, хранения и использования носителей ключевой информации с ключами ЭП и шифрования.
- К работе с СКЗИ должны допускаться только лица, прошедшие соответствующую подготовку и ознакомленные с эксплуатационной документацией на СКЗИ, а также нормативными и методическими документами по использованию ЭП.
- Рекомендуется назначить администратора безопасности, на которого возложить задачи по организации работ, связанных с использованием СКЗИ, а также контролю за соблюдением требований по безопасности.

КОНТАКТНАЯ ИНФОРМАЦИЯ

Полное наименование УЦ:
Удостоверяющий центр Общества с ограниченной ответственностью «Сампо-Сервис»
Адрес местонахождения:
197110, Санкт-Петербург, ул. Б. Разночинная д.14, лит. А, офис №115
Web-сайт: http://www.sampokey.ru
Тел..: +7(812) 640-95-60
E-Mail: uc@sampokkm.ru