Инструкция по обеспечению защиты конфиденциальной информации, обрабатываемой в автоматизированной системе «Удостоверяющий центр Федеральной службы по надзору в сфере образования и науки»

1. Общие положения

1.1. Инструкция по обеспечению защиты конфиденциальной информации, обрабатываемой в автоматизированной системе «Удостоверяющий центр Федеральной службы по надзору в сфере образования и науки» (далее – Инструкция) разработана с учетом нормативно-методических документов Федеральной службы безопасности России, а также эксплуатационной документации на сертифицированные средства криптографической защиты информации (далее - СКЗИ), используемые в автоматизированной системе «Удостоверяющий Центр Федеральной службы по надзору в сфере образования и науки» (далее - АС УЦ Рособрнадзора).

1.2. Положения настоящей Инструкции содержат общие типовые требования, которые распространяются на пользователей АС УЦ Рособрнадзора, допущенных установленным порядком к самостоятельной эксплуатации аппаратно-программных средств АС УЦ Рособрнадзора, и подлежат отражению в их должностных инструкциях.

Исходя из конкретных условий эксплуатации АС УЦ Рособрнадзора, используемых СКЗИ и персональных полномочий пользователей типовые требования могут быть конкретизированы.

1.3. Настоящая Инструкция определяет:

- требования к помещениям, в которых ведется работа с СКЗИ из состава средств защиты информации (далее – СЗИ) АС УЦ Рособрнадзора;
- обязанности пользователя, как оператора АС УЦ Рособрнадзора;
- порядок обращения с СКЗИ и ключевой информацией;
- действия при компрометации ключей.

Действие Инструкции распространяется на сертифицированные СКЗИ «КриптоПро CSP», а также на прикладные системы, построенные на основе СКЗИ и используемые в АС УЦ Рособрнадзора.

1.4. Пользователи АС УЦ Рособрнадзора допускаются к работе в АС УЦ Рособрнадзора исключительно на основании распоряжения руководителя Рособрнадзора «О допуске к обработке конфиденциальной информации в АС УЦ Рособрнадзора, после чего администраторы АС УЦ Рособрнадзора регистрируют соответствующих пользователей в АС УЦ Рособрнадзора.

К эксплуатации программно-аппаратных средств АС УЦ Рособрнадзора и СЗИ АС УЦ Рособрнадзора допускаются пользователи, прошедшие инструктаж по работе с АС УЦ Рособрнадзора и специальную подготовку по работе с СЗИ АС УЦ Рособрнадзора или обучение в иных организациях, имеющих соответствующие лицензии ФСБ России.

При допуске к работе с СКЗИ пользователь дает расписку о неразглашении конфиденциальных сведений (персональных данных), которая хранится у администратора безопасности АС УЦ Рособрнадзора или руководителя УЦ Рособрнадзора.

Если пользователь, имеющий индивидуальные ключи шифрования и (или) электронную подпись (далее – ЭП), не допущен к работе с программно-аппаратными средствами АС УЦ Рособрнадзора, то операции по шифрованию (расшифрованию) и (или) подписи электронных документов с использованием его индивидуальных ключей проводятся администратором безопасности АС УЦ Рособрнадзора в присутствии данного пользователя. На такого пользователя требования настоящей Инструкции распространяются только в части хранения и обращения с индивидуальными шифрключами.

2. Требования к помещениям, в которых ведется работа с СКЗИ

2.1. Размещение и эксплуатация СКЗИ допускается в помещениях, отвечающих требованиям документа «Инструкция по обращению с сертифицированными шифровальными средствами (средствами криптографической защиты информации)».

2.2. Порядок допуска в помещения размещения программно-аппаратных средств АС УЦ Рособрнадзора определяется документом «Инструкция о пропускном и внутриобъектовом режиме на объект информатизации – АС УЦ Рособрнадзора .

2.3. Внутренняя планировка и расположение рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им конфиденциальных документов и сведений.

2.4. В помещении, где размещены СКЗИ, запрещено использовать радиотелефоны и другую радиоаппаратуру.

2.5. По окончании рабочего дня помещения УЦ Рособрнадзора закрываются и опечатываются. Помещения УЦ Рособрнадзора с опечатанными входными дверьми сдаются под охрану установленным порядком с указанием времени приема-сдачи и с отметкой о включении охранной сигнализации в соответствующем журнале.

2.6. Перед вскрытием помещений должна быть проверена целостность оттисков печатей и исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно ставится в известность руководителя Рособрнадзора и охрану Рособрнадзора.

2.7. В случае утраты ключа от входной двери помещения УЦ Рособрнадзора, где размещены программно-аппаратные средства АС УЦ Рособрнадзора немедленно ставится в известность охрана Рособрнадзора.

3. Основные функциональные обязанности пользователя

Пользователь АС УЦ Рособрнадзора обязан:

3.1. Выполнять обязательства по всем документам, заверенным собственной ЭП, и принимать к исполнению все документы, подписанные ЭП других пользователей и признанные подлинными в соответствии с принятой в регламенте УЦ Рособрнадзора процедурой установления подлинности.

3.2. Строго соблюдать правила пользования программно-аппаратных средств АС УЦ Рособрнадзора и требования настоящей Инструкции.

3.3. Осуществлять, в рамках предоставленных полномочий, регламентные проверки при эксплуатации СКЗИ.

3.4. Не реже 1 (одного) раза в сутки проводить проверку целостности программного обеспечения СКЗИ, системного, сетевого и прикладного программного обеспечения (далее – ПО), в среде которого работают СКЗИ.

3.5. Обеспечить сохранность в тайне от посторонних лиц информации о закрепленных за ним секретных ключах шифрования и ЭП.

3.6. Своевременно принимать меры по обеспечению безопасности информации и восстановлению конфиденциальной связи в случае компрометации (подозрении в компрометации) секретных ключей.

3.7. При получении зашифрованных документов произвести их расшифрование и проверить подлинность ЭП должностных лиц отправителя, уполномоченных подписывать эти документы.

3.8. В случае обнаружения ошибки при расшифровании, либо неудовлетворительной проверки ЭП, сформировать и направить файл-уведомление об этом отправителю.

3.9. Обеспечить сохранность и конфиденциальность всей информации, которая станет ему известна при выполнении своих функций по пользованию АС УЦ Рособрнадзора.

3.10. По всем случаям выявленных отклонений в работе программно-аппаратных средств АС УЦ Рособрнадзора незамедлительно обращаться к администратору безопасности АС УЦ Рособрнадзора.

4. Порядок обращения с СКЗИ и ключевой информацией

4.1. Технические средства АС УЦ Рособрнадзора с установленными СКЗИ должны быть опечатаны печатью администратора безопасности АС УЦ Рособрнадзора.

4.2. Проверка целостности ПО СКЗИ, системного, сетевого и прикладного ПО, в среде которого работают СКЗИ, должна выполняться пользователем после загрузки операционной системы при помощи ПО контроля целостности входящего в состав ПО СКЗИ.

В случае обнаружения нарушения целостности ПО, либо повреждения печати, пользователь АС УЦ Рособрнадзора обязан незамедлительно прекратить работу и сообщить об этом администратору безопасности АС УЦ Рособрнадзора для выявления причин нарушения и принятия мер по восстановлению ПО.

4.3. Контроль сохранности входящего в состав СКЗИ технических средств АС УЦ Рособрнадзора и целости установленных на них печатей, а также всего используемого программного обеспечения для предотвращения внесения программно-аппаратных закладок и программ вирусов должен периодически проводиться администратором безопасности АС УЦ Рособрнадзора.

4.4. При эксплуатации СКЗИ не допускается:

- подключать к персональному компьютеру дополнительные устройства и соединители без соответствующего предписания на возможность их совместного использования;

- работать на персональном компьютере, если во время ее начальной загрузки не проходит встроенный тест, предусмотренный в персональном компьютере;
- оставлять без контроля вычислительные средства, входящие в состав СКЗИ, при включенном питании и загруженном программном обеспечении СКЗИ. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана производится с использованием пароля доступа;
- вносить какие-либо изменения в программное обеспечение;
- несанкционированно устанавливать создавать и выполнять на персональном компьютере посторонние программы;
- осуществлять несанкционированное вскрытие системного блока персонального компьютера.

4.5. Ключевые токены, подключаемые к порту универсальной серийной шины (далее - USB-токены) являются основным элементом, обеспечивающим стойкость конфиденциальной связи, поэтому при обращении с ключами пользователь АС УЦ Рособрнадзора должен принять все необходимые меры, направленные на исключение несанкционированного доступа к ним.

Пользователь АС УЦ Рособрнадзора обязан:

– хранить ключевые USB-токены в опечатываемом сейфе;
– не оставлять ключевые USB-токены без присмотра в дисководе компьютера или на столе;
– получать/сдавать рабочие ключевые USB-токены под роспись с указанием в журнале времени получения и сдачи;
– для восстановления ключевых USB-токенов с резервных копий обращаться с письменным заявлением к администратору безопасности АС УЦ Рособрнадзора**,** с указанием причины.

4.6. Хранение конфиденциальных документов, носителей ключевой информации, нормативной и эксплуатационной документации разрешается только в металлических шкафах (хранилищах сейфах). При вынужденных перерывах в работе ключевые USB-токеновы и другие конфиденциальные документы должны быть помещены в сейф, а сейф опечатан личной печатью. Дубликаты ключей от хранилищ хранятся в сейфе администратора безопасности АС УЦ Рособрнадзора.

Допускается хранение носителей шифрключей в одном хранилище с другими документами в условиях, исключающих их непреднамеренное уничтожение или иное не предусмотренное правилами пользования СКЗИ применение.

4.7. Для защиты ключевой информации от механических, электромагнитных и других факторов воздействия приводящих к разрушению информации, либо ее искажению целесообразно хранить USB-токеновы в футлярах из экранирующего материала.

4.8. В случае отсутствия у пользователя АС УЦ Рособрнадзора индивидуального хранилища, носители шифрключей по окончании рабочего дня должны сдаваться им лицу, ответственному за их хранение.

4.9. При работе с ключевыми USB-токенами запрещается:

а) снимать несанкционированные копии с шифрключей;

б) разглашать содержимое носителей ключевой информации или передавать сами носители лицам к ним не допущенным;

в) выводить секретные ключи на дисплей принтер или другие внешние устройства отображения информации;

г) вставлять ключевой USB-токен (или другой ключевой носитель) в USB-разъем персональной компьютер (или другое устройство считывания) в режимах, не предусмотренных штатным режимом, а также в дисководы других персональных компьютер;

д) записывать на ключевой USB-токен постороннюю информацию.

4.10. Плановая смена ключей проводиться не реже одного раза в год по инициативе руководителя УЦ Рособрнадзора.

4.11. После плановой смены ключей или компрометации ключей пользователи СКЗИ уничтожают выведенные из действия секретные ключи шифрования и ЭП со всех магнитных носителей не позднее чем через одни сутки после момента вывода ключей из действия.

Ключевая информация на носителях уничтожается администратором безопасности АС УЦ Рособрнадзора в присутствии Пользователя с использованием опции форматирования ключевого носителя штатным ПО входящего в состав АС УЦ Рособрнадзора.

Об уничтожении ключей делается соответствующая запись в «Журнале учета ключевых документов», который создается и ведется администратором безопасности АС УЦ Рособрнадзора.

5. Восстановление конфиденциальной связи после компрометации действующих ключей

5.1. Под компрометацией индивидуального ключа понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность конфиденциальной информации, циркулирующей в АС УЦ Рособрнадзора. К событиям, связанным с компрометацией действующих криптографических ключей, относятся следующие:

– утрата ключевых USB-токенов;

– утрата (в том числе хищение) ключевых USB-токенов с последующим их обнаружением;

– увольнение сотрудников, имевших доступ к ключевой информации;

– передача ключевой информации по линии связи в открытом виде (если это не предусмотрено правилами пользования);

– нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;

– возникновение подозрений на утечку информации или ее искажение;

– не расшифровывание входящих или исходящих сообщений;

– отрицательный результат при проверке электронной цифровой подписи документа;

– нарушение целостности упаковки ключевых USB-токенов и (или) печати на сейфе, где хранились ключевые USB-токены;

– несанкционированное копирование ключевых USB-токенов;

– случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе случаи, когда магнитный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате злоумышленных действий).

Первые пять событий должны трактоваться как безусловная компрометация действующих ключей, остальные - требуют специального расследования в каждом конкретном случае.

5.2. При наступлении любого из перечисленных выше событий пользователь должен немедленно прекратить связь с другими пользователями и сообщить о факте компрометации (или предполагаемом факте компрометации) администратору безопасности АС УЦ Рособрнадзора..

5.3. Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия администратором безопасности УЦ Рособрнадзора.

Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих ключей.

При установлении факта компрометации действующих ключей, скомпрометированные секретные ключи шифрования и подписи уничтожаются.

5.4. Для восстановления конфиденциальной связи после компрометации ключей Пользователь АС УЦ Рособрнадзора обращается к администратору безопасности АС УЦ Рособрнадзора с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация новых ключей шифрования и ЭП осуществляется тем же порядком, как и при плановой смене ключей.

6. Ответственность пользователя

6.1. Пользователь АС УЦ Рособрнадзора несет персональную ответственность за соблюдение правил пользования аппаратно-программными СКЗИ и требований настоящей Инструкцией**.**

6.2. Ответственность пользователя АС УЦ Рособрнадзора за неисполнение и (или) ненадлежащее исполнение своих обязанностей, предусмотренных настоящей Инструкцией, а также за разглашение имеющихся у него секретных криптографических ключей (шифрования и ЭП), другой конфиденциальной информации, ставшей ему известной при выполнении функций по пользованию АС УЦ Рособрнадзора, определяется в контракте (трудовом договоре) и обязательстве о неразглашении конфиденциальных сведений.