Приложение № 2

Утверждена

приказом _____
от «___» _____ 20___г. № _____

ИНСТРУКЦИЯ
пользователя средств криптографической защиты информации

Киров, 20__ г.

Содержание

1. Общие положения

1.1. Назначение

Настоящая инструкция содержит описание порядка организации и обеспечения функционирования сертифицированных Федеральной службой безопасности Российской Федерации средств криптографической защиты информации (далее СКЗИ), предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, обрабатываемой в информационных системах «КОГОАУ «КЭПЛ» (далее – Организация).

СКЗИ эксплуатируются в соответствии с правилами пользования ими. Изменения условий эксплуатации СКЗИ, указанных в правилах пользования ими, допускаются исключительно п согласованию с ФСБ России.

1.2. Цель разработки Инструкции

Целью настоящего Порядка является:

обеспечение защиты персональных данных с использованием средств криптографической защиты информации;

обеспечение соответствия эксплуатации СКЗИ требованиям, установленным законодательством РФ и нормативными документами.

1.3. Область применения

Настоящий документ применяется:

к рабочим местам и сервисам, в которых применяются СКЗИ;

ко всем обособленным подразделениям Организации;

ко всем офисам и удаленным сотрудникам, независимо от их местоположения.

1.4. Аудитория

Инструкция предназначена для следующих категорий сотрудников:

сотрудник, ответственный за СКЗИ (администратор СКЗИ);

пользователи СКЗИ.

Под сотрудниками в настоящей инструкции понимаются лица, состоящие в трудовых отношениях с Организацией.

Все сотрудники, в обязанности которых входит работа с СКЗИ, кроме пользователей СКЗИ, должны быть ознакомлены с инструкцией, а также с документами, на которые оно ссылается, в части их касающейся.

1.5. Нормативные ссылки

Настоящая Инструкция разработана в целях реализации следующих нормативных правовых актов:

Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных

при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

1.6. Срок действия и порядок внесения изменений в инструкцию

Инструкция действует с момента утверждения и действует бессрочно до замены новой версией или документом, его заменяющим.

Документ подлежит регулярному пересмотру с периодичностью не реже 1 раза в 3 года, а также в случае изменения требований законодательства, изменения оценки рисков информационной безопасности. Изменения в инструкцию вносятся путем издания новой версии и ознакомления с ней сотрудников.

Срок хранения после прекращения действия: постоянно.

1.7. Используемые сокращения

ПО – программное обеспечение;

ПК – персональный компьютер;

СКЗИ - средства криптографической защиты информации;

ФСБ – Федеральная служба безопасности РФ.

2. Ответственные лица

Для эксплуатации сертифицированных СКЗИ в организации назначаются лица:

администратор СКЗИ;

пользователи СКЗИ.

Функции администратора СКЗИ могут быть возложены на одного из пользователей СКЗИ, либо на структурное подразделение или работника, ответственных за безопасность конфиденциальной информации (персональных данных) или за применение средств электронной подписи. При оказании услуг по обслуживанию СКЗИ сторонней организацией, она должна обладать лицензией ФСБ на соответствующий вид работ.

Ответственные лица:

назначаются приказом по Организации и имеют функциональные обязанности в соответствии с настоящей Инструкцией;

допускаются к работе после ознакомления с настоящей Инструкцией под расписку в соответствующем журнале;

должны иметь уровень компетентности, достаточный для корректной и безопасной эксплуатации СКЗИ.

3. Обязанности пользователей СКЗИ

Пользователи СКЗИ обязаны обеспечивать:

соблюдение конфиденциальности при обращении со сведениями, которые доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документов к ним;

выполнение требований к обеспечению безопасной и корректной эксплуатации СКЗИ;

обеспечение надежного хранения СКЗИ, эксплуатационной и технической документации к ним, носителей ключевой информации;

информирование Администратора СКЗИ о ставших известными попытках посторонних лиц получить сведения об используемых СКЗИ и ключевых документах к ним.

4. Помещения ограниченного доступа с СКЗИ

Принципы организации режима в помещениях, где установлены и (или) хранятся СКЗИ, ключевые документы, эксплуатационная и техническая документация к ним (помещения):

Исключена возможность неконтролируемого проникновения в помещения.

Исключена возможность неконтролируемого пребывания посторонних лиц в помещениях.

Обеспечена сохранность конфиденциальной информации, СКЗИ, ключевых документов, эксплуатационной и технической документации к ним.

Требования к помещениям устанавливаются настоящей Инструкцией, а также эксплуатационной и технической документации на СКЗИ.

В отношении помещений с СКЗИ организацией проводятся следующие мероприятия:

назначается лицо, ответственное за помещение;

определяется перечень лиц, допущенных к работе в помещении и обслуживанию помещения;

устанавливается порядок доступа в помещение в рабочее и нерабочее время, в аварийных ситуациях (пожар, авария, стихийное бедствие и т.п.);

устанавливается порядок нахождения в помещении посторонних лиц (при необходимости их нахождения);

устанавливается порядок хранения и использования средств доступа (ключ, proximity-карта и т.п.) от помещения.

Решения по перечисленным мероприятиям определяются приказом по организации.

4.1. Требования к окнам помещений с СКЗИ

Окна помещений должны быть защищены от несанкционированного доступа посторонних лиц (в случае, если они на первом или последнем этаже, либо рядом с пожарными лестницами и другими местами, откуда возможно проникновение) металлическими решетками, ставнями или сигнализацией или другими средствами, препятствующими неконтролируемому проникновению в помещения.

Для предотвращения несанкционированного визуального просмотра помещений извне окна должны быть защищены шторами или жалюзи.

4.2. Требования к дверям помещений с СКЗИ

Двери помещений с СКЗИ должны быть оборудованы надежными замками, гарантирующими их надежное закрытие в нерабочее время.

Средства доступа от входных дверей идентифицируются (нумеруются), учитываются и выдаются сотрудникам, имеющим право доступа в помещения, под расписку в соответствующем журнале.

Дубликаты средств доступа в помещения хранятся в сейфе руководителя организации, либо администратора СКЗИ, либо другом выделенном хранилище. Режим хранения дубликатов средств доступа в помещения должен исключать неконтролируемый и необнаруживаемый доступ к ним.

В обычных условиях двери помещений могут быть открыты только сотрудниками, допущенными в них для санкционированного прохода в помещения.

Режим аварийного и нештатного доступа в помещения устанавливается соответствующим приказом по организации.

Для исключения необнаруживаемого доступа в помещения, они должны опечатываться, либо оснащаться охранной сигнализацией или системой видеонаблюдения. Мер должно быть достаточно, чтобы перед началом работы можно было определить, что проникновения в помещения не было.

4.3. Требования к техническим средствам охраны помещений с СКЗИ

Все технические средства безопасности помещений должны проходить периодический контроль работоспособности.

Помещения с СКЗИ должны быть оборудованы охранной и пожарной сигнализацией, для которых организацией установлен порядок периодической проверки их исправности.

Параметры сети электроснабжения помещений должны соответствовать требованиям инструкций по эксплуатации технических средств и правилам техники безопасности.

5. Хранение СКЗИ

За сохранность доверенных СКЗИ, ключевых носителей и документов, эксплуатационной и технической документации их пользователи несут персональную ответственность.

Хранение СКЗИ, ключевых документов, ключевых носителей, эксплуатационной и технической документации предусматривается:

для пользователя - персональные хранилища (сейфы, ящики, шкафы и т.п.), оборудованных замками, в условиях, исключающих бесконтрольный доступ к ним, а также непреднамеренное уничтожение.

Ключи от персональных хранилищ должны быть учтены и выданы пользователю под расписку.

При утрате средства доступа от хранилища или входной двери помещения необходимо либо заменить или переделать секрет замка с изготовлением и учетом новых средств доступа к нему, либо заменить хранилище или замок.

До момента изменения секрета или замены замка режим работы с этим хранилищем устанавливает администратор СКЗИ, либо руководитель организации в рамках своих полномочий.

6. Передача СКЗИ

Передача СКЗИ, дистрибутивов с СКЗИ, эксплуатационной документации к СКЗИ, ключевых носителей допускается только между пользователями СКЗИ и администратором СКЗИ. Передача между пользователями должна быть санкционирована администратором СКЗИ. Любая передача СКЗИ осуществляется под расписку в соответствующем журнале учета.

7. Аппаратные средства, функционирующие вместе с СКЗИ

Аппаратные средства, которые функционируют в штатном режиме вместе с СКЗИ должны быть:

учтены совместно с СКЗИ;

оборудованы средствами контроля за вскрытием (опечатаны или опломбированы).

При хранении ключевой информации СКЗИ в реестре Windows и на HDD персонального компьютера требования по хранению ключевых носителей распространяются на персональный компьютер. В случае невозможности отчуждения ключевого носителя с ключевой информацией от персонального компьютера организационно-техническими мероприятиями должен быть исключен несанкционированный доступ к персональному компьютеру с ключами. При хранении ключей на HDD персонального компьютера необходимо использовать парольную защиту.

Важно! Ответственность за ПК, в составе которых установленны СКЗИ и ключевая информация, несут пользователи этих ПК с момента выдачи им ПК вместе с СКЗИ или момент установки СКЗИ и допуска к работе с ПК.

8. Вывод из эксплуатации

Решение о выводе из эксплуатации и уничтожении принимается администратором СКЗИ по согласованию с руководителем организации. Не допускается нижеперечисленные действия выполнять пользователям СКЗИ.

Вывод из эксплуатации производится следующим образом:

- установленное на компьютере СКЗИ – удаление с компьютера;
- ключевые документы – надежное удаление ключевой информации с носителя;
- ключевые носители – очистка носителя;
- эксплуатационная и техническая документация к СКЗИ – хранение.

Вывод из эксплуатации осуществляется Администратором СКЗИ непосредственно в момент прекращения использования.

Удаление с компьютера СКЗИ, ключевой информации, а также других связанных с криптографией данных, должно производиться надежным образом.

После этого выполняется Администратором делается отметка в журнале учета и допускается применение компьютера в других целях.

Важно! Ключевая информация, как правило, действует в течение 1 года. Однако защищаемые с помощью её данные, чаще всего хранятся 5 и более лет, так как отражают хозяйственные, деловые или технические операции. В течение 1 года разрешается выполнять шифрование данных или их подпись. Хранение сертификатов электронной подписи должно осуществляться бессрочно.

9. Уничтожение ключевых носителей и документов

Уничтожение производится администратором СКЗИ не позднее 10 суток после вывода из эксплуатации. Факт уничтожения фиксируется в Журнале учета СКЗИ.

Уничтожение больших объемов ключевых документов и носителей может быть оформлено актом комиссией не менее двух человек из числа пользователей СКЗИ и Администратора СКЗИ. Акт утверждается руководителем организации.

Ключевые носители (диски, USB-токены) уничтожаются путем нанесения неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации на них. Непосредственные действия по уничтожению ключевых носителей регламентируются эксплуатационной и технической документацией на соответствующие СКЗИ, а также организацией, производившей запись криптоключей.

Бумажные и прочие сгораемые носители, а также эксплуатационная и техническая документация на СКЗИ уничтожается путем сжигания или с помощью бумагорезательных машин.

10. Требования к программному обеспечению на персональном компьютере с СКЗИ

За установку, настройку общесистемного, прикладного программного обеспечения и дополнительных средств защиты на персональном компьютере с СКЗИ осуществляют системный администратор и администратор СКЗИ в соответствии с правилами установки и настройки СКЗИ и программного обеспечения, изложенными в эксплуатационной и технической документации на СКЗИ.

Администратор СКЗИ должен осуществлять периодический контроль выполнения указанных требований, а также требований, приведенных в эксплуатационной и технической документации на СКЗИ.

Не допускается:

обрабатывать на персональном компьютере, оснащенном СКЗИ, информацию, содержащую государственную тайну;

осуществлять несанкционированное изменение аппаратной и программной конфигурации персонального компьютера (в том числе несанкционированное вскрытие), СКЗИ, программного обеспечения.

11. Защита СКЗИ от несанкционированного доступа

Защита компьютеров с СКЗИ обеспечивается комплексом мер:

сертифицированное ФСТЭК или ФСБ антивирусное средство;

стойкие пароли;

защита компьютера, его оборудования и носителей информации от несанкционированного доступа (в т.ч. физического): опечатывание, пароль на BIOS, минимальные привилегии пользователя.

Пользователи должны соблюдать порядок защиты от несанкционированного доступа, знать меры предосторожности при обнаружении нештатной ситуации:

сообщения об ошибках антивируса, операционной системы, прикладного программного обеспечения;

нарушения защитных пломб;

признаки проникновения в помещения и хранилища.

Пароли для однофакторной аутентификации должны формироваться в соответствии со следующими правилами:

длина пароля должна быть не менее 6 символов;

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места, числа, сочетания цифр и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

блокировка учетной записи пользователя на 30 минут после 5 неудачных попыток ввода пароля;

Пароли для двухфакторной аутентификации с использованием токенов должны формироваться в соответствии со следующими правилами:

длина пароля должна быть не менее 6 символов;

пароль может состоять из символов одной группы;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования автоматизированного рабочего места, числа, сочетания цифр и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

блокировка USB-токена после 10 неудачных попыток ввода пароля и возможность разблокировки только администратором СКЗИ.

Администратор СКЗИ, а также Пользователи СКЗИ несут персональную ответственность за обеспечение конфиденциальности паролей доступа. Запрещается записывать пароли на материальные носители и хранить их в легкодоступных местах, в том числе на мониторе, рабочем столе или ящиках стола.

Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 год. Пароль должен быть изменен раньше плановой замены в случае его компрометации. Ответственность за своевременную смену пароля несет Администратор СКЗИ.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС. Средствами BIOS должна быть исключена возможность работы на персональном компьютере СКЗИ, если во время её начальной загрузки не проходят встроенные тесты.

12. Ограничения и запреты

Пользователям запрещается:

осуществлять несанкционированное копирование ключевых носителей;

разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным

вывод ключевых документов на дисплей (монитор) персонального компьютера или принтер;

вставлять ключевой носитель в считывающее устройство в режимах, не предусмотренных штатным режимом использования ключевого носителя;

оставлять без контроля технические средства, на которых эксплуатируется СКЗИ, после ввода ключевой информации;

записывать на ключевой носитель постороннюю информацию;

использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации средствами СКЗИ.

13. Действия в случае компрометации ключей

К обстоятельствам, указывающим на возможную компрометацию криптографических ключей, относятся следующие:

потеря ключевых носителей с криптографическими ключами;

потеря ключевых носителей с криптографическими ключами с последующим их обнаружением;

увольнение работников – пользователей СКЗИ, имевших доступ к криптографическим ключам;

возникновение подозрений относительно утечки информации или её искажения;

нарушение целостности печатей на сейфах (металлических шкафах) с ключевыми носителями с криптографическими ключами, если используется процедура опечатывания сейфов;

утрата ключей от сейфов в момент нахождения в них ключевых носителей с криптографическими ключами.

Ключи шифрования, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к СКЗИ. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается, по решению администратора СКЗИ, согласованного с руководителем организации, использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшейся (хранящейся) с их использованием конфиденциальной информации (персональных данных), пользователи СКЗИ обязаны сообщать администратору СКЗИ или руководителю организации.

_____