Утверждена
распоряжением Администрации Главы
Республики Тыва и Аппарата Правительства
Республики Тыва
от « 21 » августа 2013 г. № 154-РА

Инструкция
по работе с ключевыми носителями в информационных системах обработки персональных данных

1. Общие положения

1.1. В информационных системах обработки персональных данных Администрации Главы Республики Тыва для обеспечения контроля за целостностью передаваемых по технологическим цепочкам ЭД, для подтверждения их подлинности и авторства используются средства электронной цифровой подписи, позволяющие работникам проставлять на ЭД персональные КА. Применение КА позволяет следующим в технологической цепочке работникам убедиться, что документ не искажен и подготовлен именно тем работником, кому это предписано технологическим процессом.

1.2. Каждому работнику, которому в соответствии с его функциональными обязанностями предоставлено право постановки на ЭД кодов аутентификации, выдается персональный ключевой носитель.

1.3. Для организации двухфакторной аутентификации каждому пользователю ИСПДн выдается персональный ключевой носитель.

1.4. Персональный ключевой носитель - это аппаратный носитель информации, на который записана уникальная секретная ключевая информация («секретный ключ ЭЦП», идентификатор пользователя), и предназначенная для постановки уникального кода аутентификации (КА) конкретного работника на обработанные им ЭД или для авторизации в ИСПДн.

1.5. Информация («секретный» ключ ЭЦП работника, идентификатор пользователя), находящаяся на персональном ключевом носителе, относится к категории сведений ограниченного распространения и имеет гриф «Для служебного пользования» (ДСП).

1.6. Персональный ключевой носитель изготавливается в КЦ, или при помощи СЗИ от НСД.

1.7. В Администрации Главы Республики Тыва учет и хранение персональных ключевых носителей работников осуществляет администратор информационной безопасности (при его отсутствии – начальник ИТ отдела), который ведет «Журнал

учета ключевых носителей» (Приложение №1). При изменении полномочий работника, его увольнения либо компрометации ключевого носителя уничтожается все ключевая информация, и подписывается акт об уничтожения ключевой информации с ключевых носителей (Приложение №1).
1.8. Контроль за обеспечением безопасности технологии обработки электронных документов в АС, в том числе за действиями работников, выполняющих свою работу с применением персональных ключевых носителей, осуществляется работниками ИТ отдела, ответственными за информационную безопасность.

2. Обязанности Работника

2.1. **Работник**, которому в соответствии с его должностными функциями предоставлено право постановки на ЭД персональных КА, **ОБЯЗАН**:

- Лично присутствовать при изготовлении своего персонального ключевого носителя (от момента включения до момента выключения «АРМ генерации ключей»), чтобы быть уверенным в том, что содержание его ключевых носителей не компрометировано;
- Под роспись в «Журнале учета ключевых носителей» получить ключевые носители, убедиться, что они правильно маркированы.
- Сдавать свой персональный ключевой носитель на временное хранение ответственному за информационную безопасность на время длительного отсутствия работника на рабочем месте, в период отпуска и болезни и т.п.;
- В случае порчи ключевого носителя работник обязан передать его уполномоченному работнику ИТ отдела, который в присутствии работника делает новую рабочую копию ключевого носителя. Все эти действия должны быть зафиксированы в «Журнале выдачи ключевых носителей».

2.2. Работнику ЗАПРЕЩАЕТСЯ:

- передавать свой персональный ключевой носитель другим лицам (кроме как для хранения лицу, ответственному за информационную безопасность в запечатанном конверте);
- оставлять персональный ключевой носитель без личного присмотра;
- делать неучтенные копии ключевого носителя
- подписывать своим персональным уникальным КА любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом;

- сообщать кому-либо, что он является владельцем уникального КА для данного технологического процесса.

2.3. Если у работника появилось подозрение, что его персональный ключевой носитель попал или мог попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу с ключевым носителем, сообщить об этом работнику ИТ отдела, ответственному за информационную безопасность, путем подачи заявления в службу технической поддержки, сдать ему скомпрометированный ключевой носитель, соблюдая обычную процедуру с пометкой в журнале о причине компрометации, написать объяснительную записку о факте компрометации персонального ключевого носителя на имя руководителя Администрации Главы Республики Тыва.

2.4. В случае утери персонального ключевого носителя работник обязан немедленно сообщить об этом работнику ИТ отдела, ответственному за информационную безопасность, путем подачи заявления в службу технической поддержки, написать объяснительную записку об утере носителя на имя руководителя Администрации Главы Республики Тыва и принять участие в служебном расследовании факта утери персонального ключевого носителя.

2.5. В случае перевода работника на другую работу, увольнения и т.п. он обязан сдать (сразу по окончании последнего сеанса работы) свой персональный ключевой носитель лицу, ответственному за информационную безопасность под роспись в журнале учёта ключевых носителей.

3. Ответственность

3.1. Работник несет персональную ответственность за сохранность и правильное использование вверенной ему персональной ключевой информации и содержание документов, на которых стоит его персональный код аутентификации.
3.2. За нарушение положений данной Инструкции к работнику может быть применена дисциплинарная ответственность, а так же ответственность предусмотренная действующим законодательством РФ

4. Обозначения и сокращения

АС – автоматизированной системе;

ЗАРМ – защищаемое автоматизированное рабочее место;

ВП – вредоносная программа;

ИБ – информационная безопасность;

ИСПДн – информационная система персональных данных;

КА – коды аутентификации;

КЗ – контролируемая зона;

КЦ – ключевой центр;

МЭ – межсетевой экран;

НСД – несанкционированный доступ;

ПДн – персональные данные;

ПМВ – программно-математическое воздействие;

СЗИ – средства защиты информации;

СЗПДн – система (подсистема) защиты персональных данных;

ЭД – электронные документы.

Приложение №1

Журнал
регистрации и выдачи ключевых носителей

Рег. №	Дата формирования ключевой информации	Вид ключевой информации	Наименование пользователя	Ф.И.О. администратора КЦ	Подпись	Отправлено (дд/мм/гг, подпись)	Получено (дд/мм/гг, подпись)	Уничтожено (№ акта, дд/мм/гг)
1	2	3	4	5	6	7	8	9

Утверждаю
Зам. Председателя Правительства Республики
Тыва – руководитель Администрации Главы
Республики Тыва и Аппарата
Правительства Республики Тыва
« » _____ 2013 г.

АКТ № _____
уничтожения ключевой информации с ключевых носителей

Проведено уничтожение ключевой информации с ключевых носителей :

Порядковый номер	Регистрационный номер	Вид ключевой информации (Э/Р)

С перечисленных ключевых носителей уничтожена ключевая информация посредством:
_____.
(программы _____, разрезания, сжигания)
В журнале регистрации ключевых носителей сделаны соответствующие записи.

Пользователь _____
(Ф.И.О.)

_____ _____
(Подпись) (Дата)

Администратор ИБ _____
(Ф.И.О.)

_____ _____
(Подпись) (Дата)