ПРИЛОЖЕНИЕ 8 к приказу
№___ от_____
об организационных мерах для
защиты персональных данных

ПРАВИЛА ПОЛЬЗОВАНИЯ СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

1. Общие положения

Средства криптографической защиты информации (СКЗИ), в состав которых входят средства шифрования и электронной цифровой подписи (ЭЦП), предназначены для:

- заверки файлов электронных документов, циркулирующих в системе информационного обмена электронными документами между Клиентом и Контрагентом по телекоммуникационным каналам связи, электронной цифровой подписью и подтверждения ее подлинности;
- шифрования этих файлов для закрытия содержащейся в них информации от несанкционированного просмотра при передаче по открытым каналам связи и расшифровки их при получении.

Средства шифрования и ЭЦП могут использоваться в системе информационного обмена электронными документами между Клиентом и Контрагентом по телекоммуникационным каналам связи.

2. Работа с СКЗИ и средствами ЭЦП

Для работы с СКЗИ и средствами ЭЦП привлекаются уполномоченные лица, назначенные соответствующим приказом руководителя организации. Должностные лица, уполномоченные соответствующим приказом руководителя организации эксплуатировать СКЗИ, получать и использовать ключи шифрования и ЭЦП, несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;
- сохранение в тайне содержания закрытых ключей СКЗИ и средств ЭЦП;
- сохранность носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями.

В организации должны быть обеспечены условия хранения ключевых носителей, исключающие возможность доступа к ним посторонних лиц, несанкционированного использования или копирования ключевой информации. Ключевые носители должны

храниться в сейфах индивидуального пользования.

Для исключения утраты ключевой информации вследствие дефектов носителей рекомендуется, после получения носителей с ключевой информации, создать резервные копии. Копии должны быть соответствующим образом маркированы и должны использоваться так же, как оригиналы. Должно быть обеспечено раздельное хранение действующих и резервных ключевых носителей.

Используемые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. Учет ведется администратором либо лицом, ответственным за организацию обработки и защиты ПДн в журналах установленной формы. Типовая форма журнала приведена в Приложении 1.

СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы доставляются администратором Участника при соблюдении мер, исключающих бесконтрольный доступ к ним во время доставки.

Пользователи и администратор ЛВС несут ответственность за то, чтобы на компьютере, на котором установлены СКЗИ и средства ЭЦП, не были установлены и не эксплуатировались программы (в том числе вирусы), которые могут нарушить функционирование программных СКЗИ и средств ЭЦП.

При обнаружении на рабочем месте, оборудованном СКЗИ и средствами ЭЦП, посторонних программ или вирусов, нарушающих работу указанных средств, работа со средствами защиты информации на данном рабочем месте должна быть прекращена и должны быть организованы мероприятия по анализу и ликвидации негативных последствий данного нарушения.

Не допускается:

а) разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

б) вставлять ключевой носитель в дисковод или USB считыватель ПЭВМ при проведении работ, не являющихся штатными процедурами использования ключей (шифрование/расшифровывание информации, проверка электронной цифровой подписи и т.д.), а также в дисководы или USB считыватели других ПЭВМ;

в) записывать на ключевом носителе постороннюю информацию;

г) вносить какие-либо изменения в программное обеспечение СКЗИ и средств ЭЦП;

д) использовать бывшие в работе ключевые носители для записи новой информации без предварительного уничтожения на них ключевой информации путем переформатирования (рекомендуется физическое уничтожение носителей).

Посторонние лица не должны допускаться к работе с компьютером, на котором установлены средства шифрования и ЭЦП.

Клиент несет ответственность за проведение в полном объеме организационных и технических мероприятий, обеспечивающих выполнение настоящих правил.

3. Действия в случае компрометации ключей

Под компрометацией закрытых ключей понимается:

- их утрата (в том числе с последующим обнаружением),
- хищение,
- разглашение,
- несанкционированное копирование,
- передача их по каналам связи в открытом виде,
- увольнение по любой причине сотрудника, имеющего доступ к ключевым носителям или к ключевой информации на данных носителях,
- любые другие виды разглашения ключевой информации, в результате которых закрытые ключи могут стать доступными несанкционированным лицам и (или) процессам.

При компрометации ключа у Пользователя, он должен немедленно прекратить связь по сети с другими абонентами и поставить в известность Администратора ЛВС о факте компрометации и действовать согласно Инструкции о действиях пользователей СКЗИ при компрометации криптографических ключей. Возобновление работы будет возможно только после замены скомпрометированных ключей.

4. Уничтожение ключевой информации.

Уничтожение ключевой информации с носителей разового использования производится путем, нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации.

Уничтожение ключевой информации с носителей многократного использования производится путем стирания ключевой информации без повреждения ключевого носителя (для обеспечения возможности его многократного использования). Ключевую информацию стирают по технологии, принятой для соответствующих ключевых носителей многократного использования.

Приложение №1 к правилам пользования
средствами криптографической
защиты информации

Журнал поэкземплярного учета СКЗИ

	Наименование СКЗИ	Серийный номер лицензии, дистрибутива, ключевого носителя	Отметка о получении		Отметка о выдаче		Отметка об установке СКЗИ		Отметка об изъятии СКЗИ из аппаратных средств		Примечание
			От кого	Дата	Кому	Дата и роспись в получении	Место установки	Дата и роспись лица, произведшего установку	Дата	Дата и роспись лица, произведшего изъятие	
1	2	3	4	5	6	7	8	9	10	11	12
1											
2											

Приложение №2 к правилам пользования
средствами криптографической
защиты информации

Лист ознакомления

С правилами пользования средствами криптографической защиты информации, утвержденных приказом №______________ от «   »_____________20   г. ознакомлены:

№ п/п	Ф.И.О.	Должность	ДАТА	Подпись