Утверждено
приказом директора МБОУ СОШ с.Леонидово
№ 27 от 2.02.2015г

Инструкция
о работе со средствами криптографической защиты
Информации и информационной системы персональных данных
« Сетевой город.Образование»

1.**Общие положения**
Инструкция разработана в целях повышения безопасности хранения и обработки информации ограниченного доступа (персональных данных) с использованием средств криптографической защиты информации (далее — СКЗИ), в соответствии с Федеральным законом от 27 июля 2006 года №152 «О персональных данных», приказом ФАПСИ от 13 июня 2001 года № 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», приказом ФСБ России от 09 февраля 2005 года №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» (Положение ПКЗ-2005).
Инструкция регламентирует порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи информации ограниченного доступа (персональных данных) с использованием средств криптографической защиты информации в МБОУ СОШ с.Леонидово.
Действие настоящей Инструкции распространяется на сотрудников МБОУ СОШ с.Леонидово — пользователей средств криптографической защиты информации, допущенных к работам с СКЗИ.
2.Пользователь обязан:
-Не разглашать информацию ограниченного доступа (персональные данные), обрабатываемую с помощью СКЗИ.
-Соблюдать требования по обеспечению безопасности информации ограниченного доступа с использованием СКЗИ.
-Сообщать Администратору информационной безопасности о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ.
-Немедленно уведомлять Администратора информационной безопасности о фактах утраты, нарушения целостности или работоспособности технических средств, на которых установлены СКЗИ, утраты ключей от помещений и о других фактах, которые могут привести к разглашению защищаемых сведений ограниченного доступа, а также о причинах и условиях возможной утечки таких сведений.
-Не оставлять без присмотра помещение, в котором установлены технические средства с СКЗИ.
-Следить за наличием на компьютере установленного антивирусного программного обеспечения с регулярно обновляемыми базами.
3.Администратор информационной безопасности обязан:
-В случае увольнения по любой причине сотрудника (пользователя СКЗИ), следует немедленно сменить пароль доступа к защищённой сети.
-Вести учёт используемых или хранимых СКЗИ, эксплуатационной и техническая документация к ним по установленным формам в «Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним».

-Руководствоваться требованиями «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», утвержденной Приказом ФАПСИ №152 от 13.06.2001г.

4.Пользователю запрещается:

-Выводить пароли доступа к защищённой сети на дисплей (монитор) компьютера или принтер.

-Отвечать на письма, с требованиями (просьбами, предложениями) прислать пароль доступа.

5.Ответственность пользователя:

Пароль доступа к защищённой сети относится к информации ограниченного доступа. Пользователь должен извещать Администратора ИБ обо всех случаях нарушения конфиденциальности пароля доступа.

За невыполнение или ненадлежащее выполнение обязательств по настоящей инструкции пользователь несёт ответственность в соответствии с законодательством Российской Федерации.

ЛИСТ ОЗНАКОМЛЕНИЯ С ИНСТРУКЦИЕЙ ПО РАБОТЕ С СКЗИ

№	ФИО	Дата	Подпись
1	2	3	4

Приложение к Инструкции

ПЕРЕЧЕНЬ ТЕХНИЧЕСКИХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ И ДОКУМЕНТОВ, В КОТОРЫХ ОПРЕДЕЛЕНЫ ТРЕБОВАНИЯ К СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ И НА СООТВЕТСТВИЕ КОТОРЫМ ОСУЩЕСТВЛЯЕТСЯ СЕРТИФИКАЦИЯ ИЛИ ГОСУДАРСТВЕННАЯ ЭКСПЕРТИЗА

Наименование средств криптографической защиты информации	Наименование технических нормативных правовых актов и документов, на соответствие которым осуществляется сертификация или государственная экспертиза
1	2
1. Средства шифрования	ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования" СТБ 34.101.31-2011 "Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности" Проект СТБ 34.101.27-2012 "Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации" или СТБ П 34.101.43-2009 "Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации" (задание по безопасности) СТБ 34.101.18-2009 "Информационные технологии. Синтаксис обмена персональной информацией" с учетом использования ГОСТ 28147, СТБ 34.101.31-2011 СТБ П 34.101.23-2008 "Информационные технологии. Защита информации. Форматы параметров криптографических алгоритмов" с учетом использования ГОСТ 28147, СТБ 34.101.31-2011
2. Средства электронной цифровой подписи	СТБ 1176.2-99 "Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи" СТБ 1176.1-99 "Информационная технология. Защита информации." СТБ П 34.101.45-2011 "Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи на основе эллиптических кривых" СТБ 34.101.31-2011 "Информационные технологии. Защита информации. Криптографические алгоритмы шифрования и контроля целостности" Проект СТБ 34.101.27-2012 "Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации" или СТБ П 34.101.43-2009 "Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации" (задание по безопасности)

	СТБ 34.101.17-2009 "Информационные технологии. Синтаксис запроса на получение сертификата" с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011 СТБ 34.101.18-2009 "Информационные технологии. Синтаксис обмена персональной информацией" с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011 СТБ 34.101.19-2009 "Информационные технологии. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей" с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011 СТБ П 34.101.23-2008 "Информационные технологии. Защита информации. Форматы параметров криптографических алгоритмов" с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011
3. Средства управления криптографическими ключами	СТБ 34.101.17-2009 "Информационные технологии. Синтаксис запроса на получение сертификата" с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011 СТБ 34.101.18-2009 "Информационные технологии. Синтаксис обмена персональной информацией" с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011 СТБ 34.101.19-2009 "Информационные технологии. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей" с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011 СТБ П 34.101.23-2008 "Информационные технологии. Защита информации. Форматы параметров криптографических алгоритмов" с учетом использования СТБ 1176.1-99, СТБ 1176.2-99, СТБ 34.101.31-2011 Проект СТБ 34.101.27-2012 "Информационные технологии и безопасность. Требования безопасности к программным средствам криптографической защиты информации" или СТБ П 34.101.43-2009 "Информационные технологии. Методы и средства безопасности. Профиль защиты технических и аппаратно-программных средств криптографической защиты информации" (задание по безопасности)