УТВЕРЖДАЮ
Директор МБОУ СОШ № 28
_____/ М.М.Кривчук
Приказ № «_____»
от «_____» _____ 20_____ г.

ИНСТРУКЦИЯ
по обеспечению безопасности рабочих мест обработки персональных данных МБОУ СОШ № 28

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет требования по защите рабочих мест ИСПДн, на которых ведется обработка и хранение персональных данных.

1.2. Настоящая инструкция составлена на основании требований нормативных документов ФСТЭК России.

1.3. В понятие защиты рабочих мест ИСПДн входит:

– физическая защита технических средств от несанкционированного доступа;

– парольная защита рабочих мест от несанкционированного доступа к персональных данным;

– антивирусная защита рабочих мест от несанкционированного доступа к персональным данным из сети Интернет.

2. ТРЕБОВАНИЯ ПО ЗАЩИТЕ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

В соответствии с требованиями нормативных документов ФСТЭК России методами и способами защиты информации от несанкционированного доступа являются:

2.1. реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

2.2. ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации;

2.3. разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

2.4. регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

2.5. учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

2.6. использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;

2.7. размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории;

2.8. организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных;

2.9. предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.

3. ТРЕБОВАНИЯ ПО ПАРОЛЬНОЙ ЗАЩИТЕ

3.1. С целью контроля учетных записей для доступа к информационным ресурсам персональных данных, все легализованные учетные записи ведутся в Журнале учета Логинов (Приложение 1).

3.2. Личные пароли доступа к элементам ИСПДн создаются пользователям самостоятельно.

3.3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.4. Правила формирования пароля:

– Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

– Пароль должен состоять не менее чем из 6 символов.

– В пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

– Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

– Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– Запрещается выбирать пароли, которые уже использовались ранее.

3.5. Правила ввода пароля:

– Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

– Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами.

3.6. Правила хранение пароля:

– Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

– Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.7. Лица, использующие паролирование, обязаны:

– четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

– своевременно сообщать администратору безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. ТРЕБОВАНИЯ ПО АНТИВИРУСНОЙ ЗАЩИТЕ

4.1. На каждом рабочем месте и серверах ИСПДн должно быть установлено антивирусное программное обеспечение (АВПО).

4.2. Антивирусные базы всегда должны быть в актуальном состоянии.

4.3. Запрещается работа на элементах ИСПДн с выключенным или неработоспособным АВПО.

4.4. Определение параметров и режимов работы средств антивирусного контроля осуществляется администратором безопасности (АБ) ИСПДн в соответствии с руководствами по применению конкретных антивирусных средств.

4.5. Проверка на наличие вирусов должна проводиться регулярно. Проверке подлежат:

- все файлы на жестких дисках серверов и рабочих мест;
- съемные носители, содержащие персональные данные;
- получаемые из сторонних организации файлы;
- передаваемые в сторонние организации файлы.

4.6. Результаты проверок должны фиксироваться в Журнале антивирусных проверок (Приложение 2).

4.7. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан немедленно сообщить о своих подозрениях АБ. АБ совместно с пользователем должен выполнить внеочередной антивирусный контроль.

5. ТРЕБОВАНИЯ ПО РАБОТЕ В СЕТИ ИНТЕРНЕТ

5.1. Работа в сети Интернет на элементах ИСПДн, должна проводиться при служебной необходимости.

5.2. При работе в сети Интернет запрещается:

– Осуществлять работу при отключенных средствах защиты (антивирус, межсетевой экран).

– Передавать по сети защищаемую информацию без использования средств шифрования.

– Загружать нелицензионное программное обеспечение.

– Посещать сайты сомнительной репутации (сайты содержащие нелегально распространяемое ПО и т.п.).

6. ТРЕБОВАНИЯ ПО РАБОТЕ СО СРЕДСТВАМИ ЗАЩИТЫ

6.1. На рабочих местах и серверах ИСПДн, исходя из Частной модели актуальных угроз, должны быть установлены специальные средства защиты. К ним относятся:

- межсетевые экраны;
- антивирусные средства защиты.

6.2. Все средства защиты могут быть установлены только организацией, имеющей лицензию на техническую защиту конфиденциальной информации.

6.3. Все средства защиты, установленные в ИСПДн, а также эксплуатационная документация на них, подлежат учету в Журнале учета средств защиты (Приложение 3).

6.4. Настройка средств защиты проводиться в соответствии с эксплуатационной документацией и требованиями нормативных документов ФСТЭК России.

Приложение 1

Форма Журнала учета Логинов

№	ФИО	Должность	Логин	Дата заведения	Дата удаления	Причина удаления	Подпись АБ
1							
2							
3							
4							
5							
6							
7							
8							
9							

Приложение 2

Форма Журнала учета антивирусных проверок

№	Дата проверки	Форма проверки (регулярная/внеплановая)	Проверенные АРМ	Результат проверки	Подпись АБ
1	29.01.2013	внеплановая			

Приложение 3

Форма Журнала учета СЗИ

№	Уч.№ СЗИ	Наименование СЗИ	Место установки	Дата установки	Подпись установившего	Дата изъятия	Подпись изъявшего
1							