УТВЕРЖДАЮ
Директор МБОУ «СШ №35»
_____ _Е.А. Зайцева
подпись расшифровка подписи
29 декабря 2022 г.

Инструкция пользователя муниципального бюджетного общеобразовательного учреждения «Средняя школа №35» города Смоленска

(наименование организации)

Смоленск

2022

1. Общие положения

1.1. Инструкция устанавливает обязанности пользователя муниципального бюджетного общеобразовательного учреждения «Средняя школа №35» города Смоленска по обеспечению безопасности обрабатываемых в организации персональных данных, запреты на действия пользователя, а также его права и ответственность (далее соответственно – инструкция, ИСПДн, организация).

1.2. Доступ пользователя к ИСПДн осуществляется в соответствии с перечнем сотрудников, допущенных к обработке персональных данных.

1.3. Привилегии доступа пользователя к информационным ресурсам назначаются в соответствии с матрицей прав доступа.

1.4. Контроль за исполнением требований, изложенных в инструкции, возлагается на сотрудника, ответственного за обеспечение безопасности персональных данных.

1.5. Каждый сотрудник организации, участвующий в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным, в части компетенции, в дальнейшем именуемый пользователь, несет персональную ответственность за свои действия при работе с информационными ресурсами.

2. Обязанности пользователя

2.1. Пользователь обязан:

- при работе с документами, содержащими персональные данные, руководствоваться требованиями организационно-распорядительных документов;

- строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами;

- использовать для доступа к ИСПДн собственную уникальную учетную запись (логин) и пароль;

- хранить в тайне пароли и PIN-коды, обеспечивать физическую сохранность ключевого носителя доступа к ИСПДн;

- не допускать при работе с ИСПДн просмотр посторонними лицами персональных данных, отображаемых на дисплее автоматизированного рабочего места (далее – АРМ);

- блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места;

- по вопросам, связанным с обеспечением защиты персональных данных, содержащихся в базах данных, и работе со средствами защиты информации, возникающими при работе, обращаться к администратору информационной безопасности.

2.2. Немедленно прекращать обработку персональных данных и ставить в известность администратора информационной безопасности при подозрении компрометации пароля, а также при обнаружении:

- нарушений целостности пломб, наклеек на персональной электронно-вычислительные машине (далее – АРМ), при наличии таковых, или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД);

- несанкционированных изменений в конфигурации программных или аппаратных средств АРМ;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования АРМ;

- непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств.

2.3. Немедленно информировать ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн в случае обнаружения попыток несанкционированного доступа к ИСПДн.

2.4. Немедленно информировать сотрудников, осуществляющих сетевое администрирование организации, при появлении сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или

возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов организации.

3. Действия, запрещенные пользователю

3.1. Пользователю запрещается:

- предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке;

- записывать пароль на любые носители, в том числе бумажные;

- сообщать (или передавать) посторонним лицам личные ключи или атрибуты доступа к ресурсам;

- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных;

- работать с персональными данными в присутствии посторонних (не допущенных к данной информации) лиц;

- самостоятельно изменять конфигурацию аппаратно-программных средств;

- осуществлять действия по преодолению установленных ограничений на доступ;

- отключать или изменять конфигурацию средств защиты информации;

- подключать к АРМ съемные носители информации, телефонные аппараты и иную вычислительную технику без согласования с администратором информационной безопасности и не связанную с выполнением возложенных обязанностей;

- устанавливать на АРМ программное обеспечение, не связанное с исполнением должностных обязанностей

4. Права пользователя

4.1. Пользователь имеет право:

- получать помощь по вопросам эксплуатации систем от ответственного за защиту информации;

- обращаться к сотрудникам, осуществляющим сетевое администрирование организации, по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ, необходимыми для автоматизации деятельности в соответствии с возложенными на него должностными обязанностями;

- подавать сотрудникам, осуществляющим сетевое администрирование организации, предложения по совершенствованию функционирования ИСПДн.

5. Ответственность пользователя

5.1. Пользователь несет ответственность за:

- обеспечение безопасности персональных данных при их обработке;

- нарушение работоспособности или вывод из строя системы защиты;

- преднамеренные действия, повлекшие модификацию или уничтожение персональных данных, и несанкционированный доступ к персональным данным;

- разглашение персональных данных.

5.2. За нарушение настоящей инструкции к пользователю могут применяться меры дисциплинарного воздействия.

6. Правила работы в информационно-телекоммуникационных сетях международного информационного обмена

6.1. Работа в информационно-телекоммуникационных сетях международного информационного обмена – сети Интернет и других (далее – сеть) на элементах ИСПДн должна проводиться только при служебной необходимости.

6.2. При работе в сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирусных и других);

- передавать по сети защищаемую информацию без использования средств шифрования;

- скачивать из сети программное обеспечение и другие файлы в неслужебных целях;

- посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение (ПО), сайты знакомств, онлайн игры и другие).

Лист ознакомления с инструкцией пользователя по обеспечению безопасности персональных данных МБОУ «СШ №35» города Смоленска

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления с Инструкцией	Подпись работника