УТВЕРЖДАЮ
Директор ГБОУ СО «Школа-
Интернат АОП №1 г. Саратова»

_____Л.А. Сидоренко
«20» января 2019 г.

ИНСТРУКЦИЯ

пользователя системы ИСПДН
ГБОУ СО «Школа-Интернат АОП №1 г. Саратова»

г. Саратов

2019 г.

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность пользователя ИСПДН.

1.2. Пользователь ИСПДН (далее – Пользователь) осуществляет обработку персональных данных в ИСПДН.

1.3. Пользователем является каждый сотрудник ГБОУ СО «Школы-интерната АОП №1 г. Саратова» (далее Учреждение), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты ИСПДН.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением о порядке обработке и защите персональных данных (далее – ПД), внутренними инструкциями, регламентирующими документами Учреждения и законодательством РФ.

1.5. Ознакомление сотрудников с требованиями настоящей Инструкции проводит Администратор информационной безопасности ИСПДН под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

1.6. В случае невозможности исполнения требований настоящей Инструкции в полном объеме, например:

в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний;

злоумышленных действий;

практическое исполнение настоящей Инструкции определяется администратором информационной безопасности ИСПДН, по согласованию с ответственным за обеспечение безопасности ПД Учреждения.

1.7. Ответственность за:

соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников Учреждения, использующих в работе ИСПДН.

1.8. Организация контрольных и проверочных мероприятий возлагается на Администратора информационной безопасности ИСПДН.

1.9. Инструкция подлежит:

полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДН, приводящих к существенным изменениям технологии обработки информации. Полный пересмотр данного документа проводится ответственным за обеспечение безопасности ПД Учреждения с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДН.

частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности ПД Учреждения.

1.10. Форма регистрации изменений в Инструкции представлена в Приложении 1.

1.11. Вносимые изменения не должны противоречить другим положениям Инструкции.

2. Должностные обязанности

2.1. Пользователь обязан:

2.1.1. Знать и выполнять требования, действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.1.2. Выполнять свои функциональные обязанности строго в рамках прав доступа к информационным ресурсам, техническим средствам, полученным в установленном порядке.

2.1.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, обеспечению безопасности ПД, а также руководящих и организационно-распорядительных документов.

2.2. Соблюдать требования парольной политики.

2.3. Соблюдать правила антивирусной защиты, а также других документов, регламентирующих вопросы работы в ИСПДН и обеспечение безопасности информации, в части его касающейся.

2.4. Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДН.

2.5. Немедленно ставить в известность Администратора информационной безопасности ИСПДН и ответственного за обеспечение безопасности ПД в Учреждении в случае утери личных реквизитов доступа или при подозрении компрометации личных паролей, а также:

при подозрении на совершение попыток несанкционированного доступа к автоматизированному рабочему месту (АРМ);

при обнаружении несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДН.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нём информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. При отсутствии визуального контроля за АРМ доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка> или сочетание кнопок <Windows> + L.

2.8. При обработке на АРМ защищаемой информации присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним АРМ в подразделении.

2.9. При обработке на АРМ защищаемой информации и необходимости использовать носители информации, применять только учтенные носители. Учет производится в соответствии с Инструкцией учета средств защиты и электронных носителей персональных данных.

2.10. Сотрудникам категорически ЗАПРЕЩАЕТСЯ:

Использовать компоненты программного и аппаратного обеспечения ИСПДН в неслужебных целях.

Хранить и обрабатывать личную информацию на ИСПДН.

2.11. При работе в сети Интернет:

использовать информационные ресурсы сети Интернет, содержание которых нарушает действующее законодательство Российской Федерации;

использовать информационные ресурсы сети Интернет для целей, не связанных с областью производственной деятельности пользователя;

использовать информационные ресурсы сети Интернет в личных целях.

2.12. Вносить изменения в состав и/или процесс работы внешних информационных ресурсов, если такие изменения не санкционированы собственником (владельцем) соответствующего ресурса.

2.13. Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДН или устанавливать дополнительно любые программные и аппаратные средства.

2.14. Оставлять без присмотра включенное АРМ, не активизировав средства защиты от НСД.

2.15. Оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа.

2.16. Оставлять без личного присмотра в легкодоступном месте на рабочем месте или где бы то ни было свои машинные носители и распечатки, содержащие сведения ограниченного распространения.

2.17. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты. Об обнаружении такого рода ошибок - ставить в известность Администратора информационной безопасности ИСПДН и ответственного за обеспечение безопасности ПД в Учреждении.

2.18. Записывать и хранить информацию на неучтенных носителях информации (НИ).

2.19. Оставлять во время работы магнитные НИ (или АРМ с НИ) без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации.

2.20. Отключать (блокировать) средства защиты информации (СЗИ), предусмотренные организационно-распорядительными документами;

2.21. Производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств.

2.22. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам обработки информации;

работать на АРМ при обнаружении каких-либо неисправностей;

хранить НИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;

хранить на учтенных НИ программы и данные, не относящиеся к рабочей информации;

привлекать посторонних лиц для производства ремонта АРМ.

2.23.Обо всех выявленных нарушениях, связанных с информационной безопасностью в ИСПДН, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за обеспечение безопасности ПД в Учреждении.

2.24. Для получения консультаций по вопросам работы и настройке элементов ИСПДН необходимо обращаться к Администратору информационной безопасности ИСПДН.

2.25. По всем возникающим вопросам при работе на средствах вычислительной техники (СВТ) необходимо обращаться к Администратору информационной безопасности ИСПДН.

2.26. Пользователь отвечает за правильность включения и выключения СВТ, входа в систему и все действия при работе на СВТ.

Приложение 1.

ФОРМА РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В ИНСТРУКЦИИ

ЛИСТ № ___ регистрации изменений в Инструкции

№ п.п.	Дата	Внесенное изменение	Основание (наименование, № и дата документа)	Кем внесено изменение (должность, подпись)

Лист ознакомления с

Инструкцией пользователя ИСПДН

№ п/п	Фамилия, инициалы сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении