

УПРАВЛЕНИЕ КУЛЬТУРЫ ДЕПАРТАМЕНТА ПО СОЦИАЛЬНОЙ ПОЛИТИКЕ АДМИНИСТРАЦИИ ГОРОДСКОГО ОКРУГА САРАНСК
МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ДЕТСКАЯ МУЗЫКАЛЬНАЯ ШКОЛА № 4 ИМЕНИ Л. ВОИНОВА»

430034, г. Саранск, РМ, Проспект 60 лет Октября, 12а
тел./факс: 8 (8342) 76-58-04

Приложение № 1

УТВЕРЖДАЮ:

Директор МБУДО «ДМШ № 4
им. Л. Воинова»

_____ А. Ф. Генералова
Приказ № 22 от 09.01.2018 г.

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Саранск, 2018 г.

1. Общие положения

Данная Инструкция определяет единый порядок сбора, систематизации, накопления, хранения, использования, уничтожения, защиты во время автоматизированной и неавтоматизированной обработки персональных данных (далее – ПДн) для работников МБУДО «Детская музыкальная школа № 4 имени Л. Воинова» (далее – Оператор), допущенных к обработке ПДн и перечисленных в Перечне информационных систем персональных данных.

Пользователь информационных систем персональных данных (далее – Пользователь ИСПДн) обязан хранить в тайне конфиденциальную информацию, ставшую известной ему при исполнении должностных обязанностей – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, составляющие коммерческую, врачебную, служебную тайну, тайну страхования, персональные данные, иные сведения, носящие для Оператора конфиденциальный характер, охраняемые в соответствии с законодательством РФ и нормативными документами по защите конфиденциальной информации, обработке и защите ПДн: Пользователь ИСПДн обязан пресекать действия других лиц, которые могут привести к разглашению такой информации.

ПДн не подлежат разглашению (распространению). Прекращение доступа к данным не освобождает работника от взятых им обязательств по неразглашению конфиденциальной информации.

2. Обязанности

Пользователь ИСПДн проходит обучение и инструктажи по вопросам обработки и обеспечения безопасности ПДн в объеме и порядке, установленные Администратором безопасности информационных систем персональных данных (далее – Администратор безопасности ИСПДн). Инструктаж и обучение проводят Администратор безопасности ИСПДн и Менеджер обработки персональных данных в пределах своих обязанностей. Пользователь ИСПДн в обязательном порядке должен ознакомиться со следующими документами:

- Политика в отношении обработки персональных данных;
- Документы, регламентирующие обработку и обеспечение безопасности персональных данных;
- настоящая инструкция.

Пользователь ИСПДн знает и строго выполняет правила работы со средствами защиты информации (средствами разграничения доступа, средствами антивирусной защиты), используемыми на персональных компьютерах.

Пользователь ИСПДн хранит в тайне свои данные для аутентификации (логин и пароль для входа) в информационных системах персональных данных (далее - ИСПДн), а также информацию о системе защиты, установленной в ИСПДн. Используемый пароль доступа удовлетворяет следующим условиям:

- длина пароля составляет не менее 8 символов;
- в составе символов пароля обязательно присутствуют буквы в верхнем и нижнем регистрах, цифры и специальные символы (“ ~ ! @ # \$ % ^ & * () - + _ = \ | / ? . ,);
- при смене пароля новое значение отличается от предыдущего не менее чем в 4 позициях;
- пароль может повторяться не менее чем после использования 5 различных паролей;
- пароль не включает в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков,

которые можно угадать, основываясь на информации о Пользователе ИСПДн.

В рамках организации антивирусной защиты Пользователь ИСПДн:

- контролирует факт запуска модуля антивирусной защиты после загрузки операционной системы;
- ежедневно контролирует обновление антивирусных баз на своей персональной рабочей станции;
- осуществляет антивирусный контроль любой информации, получаемой по телекоммуникационным каналам;
- осуществляет антивирусный контроль любой информации, получаемой на съемных носителях (дискетах, оптических дисках, USB flash-накопителях);
- осуществляет антивирусный контроль всей исходящей информации непосредственно перед отправкой;
- осуществляет антивирусный контроль файлов, перемещаемых в электронный архив, в частности, на файловые серверы Оператора;
- немедленно ставит в известность Администратора безопасности ИСПДн в случае подозрений на наличие вредоносных программ, а также в случае иных инцидентов, связанных с организацией антивирусной защиты.

Пользователь ИСПДн, использующий для обработки ПДн съемные носители (гибкие магнитные диски, компакт-диски, USB flash-накопители и т.д.), соблюдает порядок, установленный Регламентом учета, хранения и уничтожения носителей ПДн.

В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных средств защиты Пользователь ИСПДн ставит в известность Администратора безопасности ИСПДн.

Пользователь ИСПДн немедленно ставит в известность Менеджера обработки ПДн, Администратора безопасности ИСПДн:

- о ставших известными ему попытках разглашения конфиденциальной информации, в частности ПДн, а также о других причинах или условиях возможной утечки конфиденциальной информации;
- в случае утери носителя с ПДн или при подозрении компрометации личных ключей и паролей;
- в случае обнаружения фактов совершения в его отсутствие попыток несанкционированного доступа к персональной рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);
- в случае несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств автоматизированных систем;
- в случае возникновения иных инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн.

Пользователь ИСПДн при работе с конфиденциальной информацией принимает меры для исключения возможности визуального просмотра экрана видеомонитора лицами, не имеющими допуска к обрабатываемой информации.

Пользователю ИСПДн запрещается:

- передавать кому бы то ни было (в том числе родственникам) устно или письменно сведения, составляющие ПДн, доступ к которым он получил в связи с выполнением своих должностных обязанностей;
- использовать сведения, содержащие ПДн, которые подлежат защите,

при подготовке открытых публикаций, докладов, научных работ и т.д.;

- снимать копии или производить выписки из документов, содержащих ПДн, без разрешения руководителя;

- накапливать ненужную для работы конфиденциальную информацию, в том числе ПДн;

- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие ПДн, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами конфиденциального характера;

- использовать компоненты программного и аппаратного обеспечения автоматизированных систем подразделения в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;

- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию на неучтенных носителях информации (гибких магнитных дисках, USB-flash накопителях и т.п.);

- оставлять включенной без присмотра свою рабочую станцию, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации.

Пользователь ИСПДн предоставляет всю необходимую информацию и документы при расследовании инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн, при проведении контрольных мероприятий по защите ПДн, а также проверок со стороны регулирующих органов.

3. Права

Пользователь ИСПДн имеет право получать доступ к ПДн в количестве и объеме, требуемом для выполнения возложенных на него должностных обязанностей.

Пользователь ИСПДн имеет право обратиться за консультацией по вопросам автоматизированной и неавтоматизированной обработки ПДн в рамках выполняемого процесса обработки ПДн к Менеджеру обработки ПДн.

Пользователь ИСПДн имеет право обратиться к Администратору безопасности ИСПДн за консультацией по вопросам использования автоматизированных систем и технических средств обработки ПДн.

Пользователь ИСПДн имеет право обратиться к Администратору безопасности ИСПДн за консультацией по вопросам использования средств защиты информации, в частности ПДн, и общим вопросам обеспечения безопасности ПДн.

Пользователь ИСПДн имеет право знакомиться с проектами решений руководящего органа Оператора, касающимися порядка обработки и обеспечения безопасности ПДн.

Пользователь ИСПДн имеет право вносить на рассмотрение предложения по совершенствованию процессов обработки ПДн, в которых он принимает участие в соответствии со своими должностными обязанностями.

4. Ответственность

Пользователь ИСПДн несет ответственность за ненадлежащее соблюдение требований настоящей инструкции, а также других нормативных документов Оператора, касающихся обработки и обеспечения безопасности ПДн.

За разглашение информации ограниченного распространения, а также за

нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной предусмотренной законодательством ответственности.

5. Пересмотр и внесение изменений

Пересмотр положений настоящего документа проводится в случае рассмотрения вопросов применения новых средств и методов обработки и защиты ПДн, существенно отличающихся от применяемых у Оператора, и случаев, указанных в Регламенте по реагированию на инциденты информационной безопасности.

Инициатором пересмотра настоящей Инструкции являются Администратор безопасности ИСПДн и Менеджер обработки ПДн.

Внесение изменений производится на основании соответствующего приказа руководителя Оператора.