|  |  |
| --- | --- |
| Ешартыш шинчымашым пуышо «Йошкар-Оласе 5-шо №-ан  йоча сымыктыш школ» муниципал бюджет тöнеж | Муниципальное бюджетное учреждение дополнительного образования«Детская школа искусств № 5 г. Йошкар-Олы» |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

424918, г.Йошкар-Ола, с.Семеновка, ул.Чернышевского д.2 тел./факс: (8362) 72-78-66

E-mail: lib-5@yandex.ru

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

ОКПО 26303655, ОГРН 1031200401913, ИНН/КПП 1215085207/121501001

 **П Р И К А З**

**от 25 декабря 2017 г.** **№ 37**

**Об инструкциях обработки персональных данных**

 В целях исполнения Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»

ПРИКАЗЫВАЮ:

1. Ответственным за неавтоматизированную обработку персональных данных в информационных системах персональных данных, автоматизированную обработку персональных данных в информационных системах персональных данных, общую координацию работ по развитию сайта ознакомиться с инструкциями:

1. Пользователя информационных систем персональных данных / Приложение №1/

2. По организации антивирусной защиты /Приложение №2/

3. Пользователя ИСПДн по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций /Приложение №3/

Директор Е.П.Викторова

Ознакомлены:

Бояринцев Н.А.

Протасова Т.В.

Вагапова М.О.

Приложение №1

ИНСТРУКЦИЯ

ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. **Общие положения**

1.1. Пользователь информационных систем персональных данных (ИСПДн) (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник организации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами РФ и регламентирующими документами организации.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

1. **Должностные обязанности** Пользователь обязан:

2.1. 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.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться в администрацию организации по электронной почте или или по телефону, указанным на официальном сайте.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.9. Пользователям запрещается:

* разглашать защищаемую информацию третьим лицам;
* копировать защищаемую информацию на внешние носители без разрешения своего руководителя;
* самостоятельно устанавливать, тиражировать, или модифицировать программное

обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

* несанкционированно открывать общий доступ к папкам на своей рабочей станции;
* запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
* отключать (блокировать) средства защиты информации;
* обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
* сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
* привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций.

* 1. **Организация парольной защиты**

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

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

3.3. Правила формирования пароля:

* пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
* пароль должен состоять не менее чем из 8 символов;
* в пароле должны присутствовать символы трех категорий из числа следующих четырех: 1) прописные буквы английского алфавита от A до Z;

2) строчные буквы английского алфавита от a до z;

3) десятичные цифры (от 0 до 9);

4) 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 также 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;

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 (видеокамеры и др.).

3.5. 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.

3.6. Лица, использующие паролирование, обязаны:

* четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
* своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.
	1. **Правила работы в сетях общего доступа и (или) международного обмена**

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

* осуществлять работу при отключенных средствах защиты (антивирус и других);
* передавать по Сети защищаемую информацию без использования средств шифрования;
* запрещается скачивать из Сети программное обеспечение и другие файлы;
* запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
* запрещается нецелевое использование подключения к Сети.
	1. **Права и ответственность пользователей ИСПДн**

5.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн.

5.2. Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. N 152-ФЗ "О персональных данных" и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Приложение №2

**ИНСТРУКЦИЯ**

**ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ**

1. Настоящая Инструкция определяет требования к организации защиты от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников организации за их выполнение.
2. К использованию в организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.
3. Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником организации. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.
4. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.
5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).
6. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитора»). Полная проверка информации, хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.
7. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться еженедельно.
8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения)

программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка:

* на защищаемом автоматизированном рабочем месте (АРМ) - ответственным за обеспечение информационной безопасности.

1. 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.) сотрудник организации самостоятельно или вместе с ответственным за антивирусную защиту организации должен провести внеочередной антивирусный контроль своей рабочей станции.

2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

* приостановить работу;
* немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за антивирусную защиту организации, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;
* совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
* провести лечение или уничтожение зараженных файлов.
1. Ответственность за антивирусный контроль в организации, в соответствии с требованиями настоящей Инструкции возлагается на руководителя организации.
2. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за антивирусную защиту и всех сотрудников, являющихся пользователями ПК.
3. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками осуществляется ответственным за антивирусную защиту организации.

Приложение №3

 **ИНСТРУКЦИЯ**

**ПОЛЬЗОВАТЕЛЯ ИСПДН ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ВОЗНИКНОВЕНИИ ВНЕШТАТНЫХ СИТУАЦИЙ**

 **Назначение и область действия**

1.1. Настоящая инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн организации, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания в случае реализации рассматриваемых угроз.

1.3. Задачей настоящей Инструкции является:

* определение мер защиты от прерывания;
* определение действий восстановления в случае прерывания.

1.4. Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также на основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

* системы жизнеобеспечения;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

 **Порядок реагирования на аварийную ситуацию**

1. **Действия при возникновении аварийной ситуации**
2. В настоящем документе под аварийной ситуацией понимается некоторое

происшествие, связанное со сбоем в функционировании элементов ИСПДн пользователям ИСПДн. Аварийная ситуации становится возможной в результате реализации одной из угроз, приведенных в таблице «Источники угроз».

|  |  |
| --- | --- |
|  | **Источники угроз** |
|  |  |
|  | **Технологические угрозы** |
| 1 | Пожар в здании |
| 2 | Повреждение водой (прорыв системы водоснабжения, канализационных труб, систем |
|  | охлаждения) |
| 3 | Взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под |
|  | давлением) |
| 4 | Химический выброс в атмосферу |
|  | **Внешние угрозы** |
| 5 | Массовые беспорядки |
| 6 | Сбои общественного транспорта |
| 7 | Эпидемия |
| 8 | Массовое отравление персонала |
|  | **Стихийные бедствия** |
| 9 | Удар молнии |
| 10 | Сильный снегопад |
| 11 | Сильные морозы |
| 12 | Просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением |
|  | здания |
| 13 | Затопление водой в период паводка |
| 14 | Наводнение, вызванное проливным дождем |
| 15 | Подтопление здания (воздействие подпочвенных вод, вызванное внезапным и |
|  | непредвиденным повышением уровня грунтовых вод) |
|  | **Телекоммуникационные и ИТ угрозы** |
| 16 | Сбой системы кондиционирования |
| 17 | Сбой ИТ – систем |
|  | **Угроза, связанная с человеческим фактором** |
| 18 | Ошибка персонала, имеющего доступ к серверной |
| 19 | Нарушение конфиденциальности, целостности и доступности конфиденциальной |
|  | информации |
|  | **Угрозы, связанные с внешними поставщиками** |
| 20 | Отключение электроэнергии |
| 21 | Сбой в работе Интернет-провайдера |
| 22 | Физический разрыв внешних каналов связи |

2.1.2. Все действия в процессе реагирования на аварийные ситуации должны документироваться ответственным за реагирование сотрудником в «Журнале по учету мероприятий по контролю».

2.1.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники организации (Администратор безопасности, Администратор и Оператор ИСПДн) предпринимают меры по восстановлению работоспособности системы. Принимаемые меры по возможности согласуются с вышестоящим руководством. По мере

необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

**2.2. Уровни реагирования на инцидент**

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

**Уровень 1 – Незначительный инцидент.** Незначительный инцидент определяетсякак локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование сотрудниками.

* **Уровень 2 – Авария.** Любой инцидент,который приводит или может привести кпрерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки управления ответственными за реагирование сотрудниками.

К авариям относятся следующие инциденты:

1. Отказ элементов ИСПДн и средств защиты из-за:

- повреждения водой (провыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или проливных дождей; - сбоя системы кондиционирования.

2. Отсутствие Администратора ИСПДн и Администратора безопасности более чем на сутки из-за:

- химического выброса в атмосферу; - сбоев общественного транспорта; - эпидемии; - массового отравления персонала;

- сильного снегопада; - сильных морозов.

* **Уровень 3 – Катастрофа.** Любой инцидент,приводящий к полному прерываниюработоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относятся обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты: - пожар в здании; - взрыв;

- просадка грунта с частичным обрушением здания;

- массовые беспорядки в непосредственной близости от объекта.

* 1. **Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций**

**3.1.Технические меры**

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения и возникновения аварийных ситуаций, такие как:

* системы жизнеобеспечения;
* системы обеспечения отказоустойчивости;
* системы резервного копирования и хранения данных;
* системы контроля физического доступа.

Системы жизнеобеспечения ИСПДн включают:

* пожарные сигнализации и системы пожаротушения;
* системы вентиляции и кондиционирования;
* системы резервного питания.

3.1.2. Все критические помещения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.1.3. Порядок предотвращения потерь информации и организации системы жизнеобеспечения ИСПДн описан в Порядке резервирования и восстановления работоспособности технических систем и программного обеспечения, баз данных и средств защиты информации.

**3.2. Организационные меры**

3.2.1. Ответственные за реагирование сотрудники ознакомляют всех остальных сотрудников, находящихся в их зоне ответственности, с данной Инструкцией в срок, не превышающий трех рабочих дней с момента выхода нового сотрудника на работу. По окончании ознакомления сотрудник расписывается в листе ознакомления. Подпись сотрудника должна соответствовать его подписи в документе, удостоверяющем его личность.

3.2.2. Должно быть проведено обучение должностных лиц организации, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

* оказание первой медицинской помощи;
* пожаротушение;
* эвакуация людей;
* защита материальных и информационных ресурсов;
* методы оперативной связи со службами спасения и лицами, ответственными за реагирование на аварийную ситуацию;
* выключение оборудования, электричества, водоснабжения.

3.2.3. Администраторы ИСПДн и Администраторы безопасности должны быть дополнительно обучены методам частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации.