СОГЛАСОВАНО

Председатель профкома

_____ О.М. Баландина

« ___ » _____ 2018 г.

УТВЕРЖДАЮ

Директор МОУ-СОШ №1

_____ Л.П. Карманова

« ___ » _____ 2018 г.

Подписан: Карманова Лидия Прокопьевна
DN: C=RU, O=МОУ-СОШ №1 г. Петровск-Забайкальский, CN=Карманова Лидия Прокопьевна, E=school-1-pzb@mail.ru
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: г. Петровск-Забайкальский
Дата: 2022.04.15 12:04:04+09'00'

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ

информационной системы МОУ-СОШ №1

2018 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция пользователя информационной системы МОУ-СОШ №1 (далее – Инструкция) разработана в соответствии с требованиями следующих документов:

– Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждены приказом ФСТЭК России от 11 февраля 2013 г. №17.

– Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства РФ от 15.09.2008 № 687;

– Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержден приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21.

1.2. Настоящая Инструкция определяет задачи, функции, обязанности, права и ответственность пользователя, допущенного к работе на штатных средствах информационной МОУ-СОШ №1 (далее – ИС, ИСПДн).

1.3. Пользователь должен иметь допуск к работе с персональными данными в ИСПДн, в соответствии с приказом руководителя и входить в Список должностных лиц, имеющих доступ к информационной системе МОУ-СОШ №1.

1.4. Пользователь ИСПДн (он же пользователь информационной системы МОУ-СОШ № 1) при выполнении работ в пределах своих функциональных обязанностей обеспечивает безопасность обрабатываемой и хранимой в ИСПДн информации.

1.5. Перед началом обработки персональных данных в ИСПДн, пользователь должен ознакомиться с требованиями настоящей Инструкции, нормативными документами, регламентирующими вопросы защиты персональных данных, а также пройти инструктаж по требованиям эксплуатационных документов (ЭД) на системы защиты информации от несанкционированного доступа (СЗИ НСД), технические и программные средства ИСПДн.

1.6. Выдача паролей и ключей для СЗИ НСД, а также контроль за действиями пользователя и обслуживающего персонала ИСПДн осуществляется администратором безопасности информации.

2. ОСНОВНЫЕ ЗАДАЧИ И ФУНКЦИИ ПОЛЬЗОВАТЕЛЕЙ

2.1. Основными задачами пользователей являются:

– выполнение работ в соответствии со служебными (должностными) обязанностями в рамках полученного задания.

2.2. Основными функциями пользователей являются:

– обработка персональных данных в рамках служебных (должностных) обязанностей;

– обеспечение функционирования средств и систем защиты информации в пределах возложенных на него обязанностей;

3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

3.1. Хранить в тайне информацию, не составляющую государственную тайну (далее – персональные данные, конфиденциальная информация), ставшую известной при выполнении служебных (должностных) обязанностей в процессе работы в ИСПДн.

3.2. Хранить в тайне персональные идентификаторы и пароли, используемые для входа в ИСПДн.

3.3. При обработке информации, руководствоваться правилами работы с общесистемным и прикладным программным обеспечением, средствами защиты информации, средствами антивирусной защиты, используемыми в ИСПДн.

3.4. Исключать возможность несанкционированного ознакомления с отображаемыми на экране видеомонитора персонального рабочего места пользователя конфиденциальной информацией субъектами, не допущенными для обработки данной информации.

3.5. Для хранения персональных данных в случае необходимости, обусловленной технологическими особенностями их обработки, обусловленными особенностями функциональных (должностных обязанностей) использовать только учтенные установленным порядком машинные носители конфиденциальной информации (далее – МНИ).

3.6. При выходе в течение рабочего дня из помещения, где расположено персональное рабочее место пользователя, убирать документы, содержащие персональные данные, и МНИ в сейф (или запираемый шкаф), исключающий возможность несанкционированных действий злоумышленников (несанкционированное использования, копирования, ознакомления, уничтожения или хищение).

3.7. Для предотвращения НСД к информации, в свое отсутствие пользователи обязаны выключать персональную электронно-вычислительную машину (ПЭВМ) или блокировать ее.

3.8. Соблюдать правила работы с СЗИ и установленный режим разграничения доступа к техническим средствам, программам, данным, файлам с конфиденциальной информацией.

3.9. Докладывать администратору безопасности информации или лицу, его замещающему, о всех инцидентах информационной безопасности, фактах несанкционированного доступа, случаях утечки и модификации информации, обрабатываемой в ИСПДн.

3.10. Использовать только штатные программные и технические средства.

3.11. Установка новых программных и технических средств, должна быть вызвана исключительно целями повышения эффективности реализации возложенных на пользователя функциональных (должностных) обязанностей по работе с персональными данными. Возможность установки новых программных и технических средств должна согласовываться с администратором безопасности информации.

3.12. Использовать средство антивирусной защиты в соответствии с требованиями ЭД на него и соответствующей инструкции. Проводить обязательную проверку получаемых из других структурных подразделений или из сторонних организаций МНИ средствами антивирусной защиты перед копированием или запуском информации с них.

3.13. При появлении сообщений или предупреждений об обнаружении программ-вирусов или других вредоносных программ в оперативной памяти персонального автоматизированного рабочего места, зараженных файлов на внутренних или внешних носителях информации, пользователь обязан незамедлительно прекратить работу, сообщить о случившемся событии администратору безопасности информации и действовать в соответствии с полученными инструкциями.

3.14. Производить выключение питания ПЭВМ, после завершения своей работы при помощи стандартной процедуры ОС Windows «Завершение работы».

3.15. Принимать меры по реагированию, в случае возникновения нештатных и аварийных ситуаций, с целью их предотвращения или ликвидации их последствий, в рамках возложенных него функций.

3.16. Своевременно сообщать администратору безопасности информации об утере, компрометации, несанкционированном изменении персонального пароля.

4. ПРАВА ПОЛЬЗОВАТЕЛЯ

4.1. Пользователь имеет право:

– обращаться к администратору безопасности информации с просьбой об оказании технической и методической помощи по обеспечению безопасности информации, обрабатываемой на персональном рабочем месте;

– обращаться к администратору безопасности информации с требованием о прекращении обработки персональных данных, в случаях нарушения установленной технологии их обработки или нарушения функционирования средств и систем защиты информации.

5. ПОЛЬЗОВАТЕЛЮ ЗАПРЕЩАЕТСЯ

5.1. Использовать нештатные технические средства и системы для обработки персональных данных, самостоятельно вносить изменения в состав, конфигурацию, и размещение персонального автоматизированного рабочего места, входящего в состав ИСПДн.

5.2. Использовать нештатные программные средства, самостоятельно вносить изменения в состав программных средств персонального автоматизированного рабочего места.

5.3. Записывать персональный пароль на любые неучтенные носители информации, предметы мебели и технические средства (клавиатуру, монитор и пр.), сообщать его устно или письменно посторонним лицам.

5.4. Производить копирование документов, массивов данных, содержащих персональные данные, на неучтенные носители информации.

5.5. Проводить обработку персональных данных, при неисправно работающих средствах защиты информации, обрабатывать информацию в случае, если имеют место неисправности, создающие предпосылки для утечки персональных данных.

5.6. Допускать к работам в ИСПДн (на персональном автоматизированном месте) лиц, не имеющих допуска к этим работам, без согласования с ответственным за обеспечение безопасности персональных данных.

5.7. Несанкционированно тиражировать, передавать и модифицировать программные СЗИ.

5.8. Пользователям категорически запрещается бесконтрольно оставлять персональное автоматизированное рабочее место, не выполнив требования п.п. 3.7 настоящей Инструкции.

5.9. Подключать к персональному автоматизированному рабочему месту личные внешние носители и мобильные устройства.

5.10. Привлекать посторонних лиц для производства ремонта или настройки персонального автоматизированного рабочего места, без согласования с администратором безопасности информации.

6. ТЕХНОЛОГИЯ РЕШЕНИЯ ОСНОВНЫХ ЗАДАЧ И ВЫПОЛНЕНИЯ СВОИХ ФУНКЦИОНАЛЬНЫХ ОБЯЗАННОСТЕЙ ПОЛЬЗОВАТЕЛЕМ

6.1. При обработке персональных данных пользователь:

6.1.1. После загрузки операционной системы пользователь использует диалоговый интерфейс Windows, где вводит (предъявляет) текущее имя пользователя (идентификатор) и пароль для входа в систему.

6.1.2. Далее запускает штатные программные средства, входящие в состав штатного программного обеспечения персонального автоматизированного рабочего места, в целях обработки персональных данных и выполнения функциональных (должностных) обязанностей, выполняет действия, исполняет документы в соответствии со служебной необходимостью.

6.2. Своевременную смену пароля пользователь осуществляет самостоятельно, с учетом требований п.7 «Положения о защите персональных данных, обрабатываемых в информационной системе МОУ-СОШ №1.

6.3. Для проверки МНИ, каталогов или файлов на отсутствие вредоносных программ (вирусов) пользователь использует штатные средства антивирусной защиты.

7. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ

7.1 Пользователи несут ответственность в полном объеме за:

– разглашение персональных данных, ставших известными им в ходе выполнения функциональных (должностных) обязанностей, а также утрату учтенных МНИ и бумажных носителей (документов) с персональными данными;

– правильность и полноту выполнения целей, задач, функций, прав и обязанностей по защите персональных данных, возложенных на него;

– невыполнение указаний администратора безопасности информации;

– незнание и несоблюдение установленных в организации требований по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных, а также руководящих и организационно-распорядительных документов, регламентирующих обработку персональных данных в части касающейся;

– компрометацию персонального пароля, его разглашение, запись или нанесение на технические средства и неучтенные установленным порядком.

7.2 Любое нарушение требований настоящей Инструкции должно фиксироваться, а по фактам грубых нарушений должны проводиться служебные расследования (проверки). При

установлении виновных в нарушениях, мера ответственности должна определяться серьезностью и систематичностью нарушений, преднамеренностью действий и другими факторами и должна быть адекватной причиненному ущербу.

7.3 Информация о действиях пользователя, угрожающего безопасности и интересам организации, может быть передана в правоохранительные органы.

Лист ознакомления с инструкцией

№ п/п	Ф.И.О.	Дата ознакомления с инструкцией	Подпись	Примечание
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				

№ п/п	Ф.И.О.	Дата ознакомления с инструкцией	Подпись	Примечание
27.				
28.				
29.				
30.				
31.				
32.				
33.				
34.				
35.				
36.				
37.				
38.				
39.				
40.				
41.				
42.				
43.				
44.				
45.				
46.				
47.				
48.				
49.				
50.				
51.				
52.				
53.				

№ п/п	Ф.И.О.	Дата ознакомления с инструкцией	Подпись	Примечание
54.				
55.				
56.				
57.				
58.				
59.				
60.				
61.				
62.				
63.				
64.				
65.				
66.				
67.				
68.				
69.				
70.				
71.				
72.				
73.				
74.				
75.				
76.				
77.				
78.				
79.				