Краевое государственное казенное общеобразовательное учреждение, реализующее адаптированные основные общеобразовательные программы «Школа № 4»

ПРИКАЗ

_28.01.2022___ г. Амурск № 20\1Д

О назначении уполномоченного
за организацию обработки
персональных данных в КГКОУ
«Школа № 4»

В целях исполнения Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», Приказа ФСТЭК России от 11 февраля 2013 г. N 17«Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных в Краевом государственном казенном общеобразовательном учреждении, реализующим адаптированные основные общеобразовательные программы «Школа № 4» специалиста по защите информации, Неверова Романа Николаевича.

2. Ответственному за организацию обработки персональных данных обеспечить автоматизированную обработку персональных данных на объектах информатизации, удовлетворяющих действующему законодательству.

3. Утвердить инструкцию ответственного за организацию обработки персональных данных (приложение 1).

4. Ответственному за организацию обработки персональных данных руководствоваться инструкцией ответственному за организацию обработки персональных данных.

5. Ответственному за организацию обработки персональных данных обеспечить неавтоматизированную обработку персональных данных в соответствии с действующим законодательством.

6. Администратором безопасности информации в Краевом государственном казенном общеобразовательном учреждении, реализующим адаптированные основные общеобразовательные

программы «Школа № 4» назначить специалиста по защите информации, Неверова Романа Николаевича.

7. Утвердить прилагаемую инструкцию пользователя ИС. (приложение 2).

8. Утвердить прилагаемую инструкцию администратора безопасности. (приложение 3).

9. Утвердить прилагаемую инструкцию по организации парольной защиты в информационных системах персональных данных (приложение 4).

10. Утвердить прилагаемую инструкцию по организации антивирусной защиты (приложение 5).

11. Администратору безопасности в своей работе руководствоваться инструкцией администратора безопасности в Краевом государственном казенном общеобразовательном учреждении, реализующим адаптированные основные общеобразовательные программы «Школа № 4»

12. Администратору безопасности организовать проведение работ по защите информации в соответствии с руководящими документами ФСТЭК России и ФСБ России.

13. Лицам, допущенным к обработке персональных данных при неавтоматизированной их обработке и хранении руководствоваться документом «Правила обработки персональных данных без использования средств автоматизации».

14. Лицам, допущенным к обработке персональных данных при автоматизированной их обработке и хранении руководствоваться следующими документами:

- политика информационной безопасности;
- инструкция пользователя ИС.
- Инструкцией по организации парольной защиты

15. Контроль за исполнением настоящего приказа оставляю за собой.

Директор школы О.И. Лебедева

Ознакомлены:

Краевое государственное казенное общеобразовательное учреждение,
реализующее адаптированные основные общеобразовательные программы
«Школа № 4»

Приложение 1

УТВЕРЖДЕНО
приказом директора школы
от 28.01.2022. № 20\1Д

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в
Краевом государственном казенном общеобразовательном учреждении,
реализующим адаптированные основные общеобразовательные программы
«Школа № 4»

г. Амурск
2022 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за организацию обработки персональных данных в КГКОУ Школа 4 (далее – Ответственный) назначается приказом руководителя КГКОУ Школа 4 (далее – Учреждение) и отвечает за организацию, обеспечение своевременного и квалифицированного выполнения сотрудниками Учреждения законодательства Российской Федерации о персональных данных (далее – ПДн), в том числе требований к обработке и защите ПДн.

1.2. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и защиты ПДн.Ответственный поддерживает в актуальном состоянии свои знания в сфере действующего законодательства и законодательных инициатив, связанных с защитой персональных данных.

1.3. В своей деятельности Ответственный руководствуется Положением об обработке и защите персональных данных, настоящей Инструкцией и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.

2. ОСНОВНЫЕ ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по организации обработки ПДн при решении следующих основных вопросов:

- организация доступа к ПДн и учет сотрудников Учреждения, допущенных к обработке ПДн, как в программных комплексах, входящих в состав ГИС, так и на бумажных носителях;
- контроль за поддержанием в актуальном состоянии действующих локальных нормативных актов, журналов и форм учета по работе с ПДн;
- контроль за обеспечением соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;

- организация работы по заключению договоров на работы по защите ПДн;
- контроль изменений в процессах обработки ПДн и, в случае необходимости, отправка информации об этих изменениях в уполномоченный территориальный орган по защите прав субъектов персональных данных (Роскомнадзор) с целью актуализации уведомления КГКОУ Школа 4 в реестре операторов ПДн;
- рассмотрение предложений по совершенствованию действующей системы защиты ПДн, предоставленных Администратором, назначаемым приказом руководителя {Название Организации};
- осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

3. ОСНОВНЫЕ ОБЯЗАННОСТИОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Знать цели обработки ПДн в Учреждении и перечень обрабатываемых ПДн.

3.2. Соблюдать требования нормативных актов Учреждения, устанавливающих порядок работы с ПДн.

3.3. Обеспечивать доведение до сведения сотрудников Учреждения законодательства Российской Федерации о ПДн, нормативных актов по вопросам обработки ПДн, требований к защите ПДн.

3.4. Осуществлять внутренний контроль за соблюдением сотрудниками Учреждения законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

3.5. Контролировать ведение документации, предусмотренной нормативными актами Учреждения в части обеспечения безопасности ПДн.

3.6. Обеспечивать доработку локальных нормативных документов по защите ПДн Учреждения в случае такой необходимости или при поступлении такого требования от регулирующего органа.

3.7. Участвовать в расследовании нарушений по вопросам защиты ПДн, имевших место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений.

3.8. Обеспечивать организацию проведения занятий со специалистами Учреждения по организационным вопросам обработки ПДн (проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в Учреждении).

3.9. Обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов согласно п.3 ч.4 ст.22.1 Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных».

4. ПРАВА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Знакомиться с документами и материалами, необходимыми для выполнения возложенных на него задач.

4.2. Проводить проверки соблюдения режима обеспечения безопасности ПДн в структурных и (или) территориальных подразделениях Учреждения (при их наличии) в соответствии с утвержденным приказом руководителя {Название Организации} планом мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в ГИС «Бухгалтерия и кадры».

4.3. Требовать от сотрудников Учреждения соблюдения требований нормативно-правовых и организационно-распорядительных документов по вопросам обработки ПДн.

4.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обработки ПДн.

4.5. Требовать от сотрудников Учреждения письменных объяснений при проведении служебных расследований по вопросам нарушений требований по обработке и защите ПДн.

4.6. Вносить предложения руководителю{Название Организации} об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по обработке и защите ПДн.

4.7. Давать сотрудникам Учреждения обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации и локальными нормативными актами Учреждения.

4.8. Привлекать в установленном порядке специалистов Учреждения, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.

Краевое государственное казенное общеобразовательное учреждение,
реализующее адаптированные основные общеобразовательные программы
«Школа № 4»

Приложение 2

УТВЕРЖДЕНО
приказом директора школы
от 28.01.2022. № 20\1Д

ИНСТРУКЦИЯ
пользователя информационных систем

Содержание

1. Общие положения 10
2. Функции и обязанности пользователя ИС 10
3. Порядок пересмотра инструкции 12
4. Ответственные за организацию и контроль выполнения инструкции 13
Приложение 1 – Лист регистрации изменений 14
Приложение 2 – Лист ознакомления 15

1. Общие положения

Ознакомление сотрудников КГКОУ Школа 4 с требованиями настоящей Инструкции проводит администратор информационной безопасности информационной системы персональных данных под подпись с выдачей электронных копий Инструкции непосредственно для повседневного использования в работе.

2. Функции и обязанности пользователя ИС

Каждый сотрудник КГКОУ Школа 4 участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки защищаемой информации (в т.ч. персональных данных) и имеющий доступ к аппаратным средствам, программному обеспечению и данным, содержащимся в ИС, несет персональную ответственность за свои действия и обязан:

– строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС;

– выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам, техническим средствам, полученным в установленном порядке;

– знать и строго выполнять правила работы со средствами защиты информации, установленными в ИС;

– хранить в тайне свой пароль (пароли);

– исполнять требования «Порядка парольной защиты в ИС», «Инструкции по организации антивирусной защиты ИС», а также других документов, регламентирующих вопросы работы в ИС и обеспечения безопасности информации в части, его касающейся;

– немедленно ставить в известность АИБ ИС и начальника отдела в случае утери личных реквизитов доступа, при компрометации личных

паролей, подозрении на совершение попыток несанкционированного доступа (НСД) к персональным электронно-вычислительным машинам, обнаружении несанкционированных изменений в конфигурации программных или аппаратных средств ИС;

– немедленно ставить в известность администратора ИС при обнаружении отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИС, выхода из строя или неустойчивого функционирования устройств ПЭВМ (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных ТС защиты информации;

– при обработке на ПЭВМ защищаемой информации присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним ПЭВМ в отделе;

– при обработке на ПЭВМ защищаемой информации и необходимости использовать носители информации, применять только учтенные носители.

Сотрудникам ЗАПРЕЩАЕТСЯ:

– использовать компоненты программного и аппаратного обеспечения ИС в неслужебных целях;

– хранить и обрабатывать личную информацию на ПЭВМ и серверах ИС;

– 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;

•вносить изменения в состав и/или процесс работы внешних информационных ресурсов, если такие изменения не санкционированы собственником (владельцем) соответствующего ресурса;

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

– оставлять без присмотра включенную ПЭВМ, не активизировав средства защиты от НСД;

– оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа;

– 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;

– использовать в работе неучтенные носители информации для обработки защищаемой информации;

– умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты, об обнаружении такого рода ошибок – ставить в известность АИБ ИС и начальника своего отдела.

3. Порядок пересмотра инструкции

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИС КГКОУ Школа 4 приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности и обработки персональных данных КГКОУ Школа 4.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности и обработки ПДн КГКОУ Школа 4 целью

проверки соответствия положений данного документа реальным условиям применения их в ИС КГКОУ Школа 4.

Форма регистрации изменений в Инструкции представлена в Приложении 1.

Вносимые изменения не должны противоречить другим положениям Инструкции.

4. Ответственные за организацию и контроль выполнения инструкции

Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников КГКОУ Школа 4 участвующих в обработке защищаемой информации (в том числе персональных данных).

Ответственность за организацию контрольных и проверочных мероприятий возлагается на АИБ ИС.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности и обработку персональных данных.

Приложение 1 – Лист регистрации изменений

Лист регистрации изменений в инструкции

№ п/п	Внесенное изменение	Основание (наименование, номер и дата документа)	Лицо, внесшее изменения		Дата внесения изменения
			Фамилия, инициалы	Подпись	

Приложение 2 – Лист ознакомления

Лист ознакомления

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

Краевое государственное казенное общеобразовательное учреждение,
реализующее адаптированные основные общеобразовательные программы
«Школа № 4»

Приложение 3

УТВЕРЖДЕНО
приказом директора школы
от 28.01.2022. № 20\1Д

ИНСТРУКЦИЯ
администратору информационной безопасности

г. Амурск
2022 год

Данная инструкция определяет круг задач, основные права и обязанности администратора информационной безопасности Краевое государственное казенное общеобразовательное учреждение, реализующее адаптированные основные общеобразовательные программы "школа № 4" (далее по тексту — КГКОУ Школа 4).

Общие положения:

1.Назначение на должность администратора информационной безопасности, закрепление за данным лицом определенных полномочий и обязанностей производится приказом Директора КГКОУ Школа 4.

2.В своей деятельности администратор информационной безопасности руководствуется требованиями действующего законодательства Российской Федерации и внутренних документов КГКОУ Школа 4 по вопросам защиты информации, обеспечивает их выполнение в КГКОУ Школа 4.

3.Администратор информационной безопасности непосредственно подчиняется директору КГКОУ Школа 4 и, помимо обязанностей, закрепленных настоящей Инструкцией, исполняет его указания и распоряжения в рамках выполнения своих основных задач.

4.Основные задачи администратора информационной безопасности:

ведение и актуализация перечня работников КГКОУ Школа 4, имеющих доступ к персональным данным (далее по тексту – ПДн), обрабатываемым в КГКОУ Школа 4;

•оценка угроз безопасности ПДн, обрабатываемых в информационных системах персональных данных (далее по тексту – ИСПДн) КГКОУ Школа 4, и их источников;

•участие в выборе методов и способов защиты ПДн, обрабатываемых в ИСПДн, формирование требований по обеспечению безопасности ПДн с помощью технических методов защиты;

•участие в проектировании системы защиты персональных данных (далее по тексту – СЗПДн) и внедрении средств защиты информации, взаимодействие с подрядными организациями, привлеченными для выполнения данных работ;

•мониторинг функционирования средств защиты информации;

•участие в реагировании на инциденты информационной безопасности, связанные с нарушением заданных характеристик безопасности ПДн, обрабатываемых в ИСПДн;

•обеспечение соблюдения требований по безопасности информации при эксплуатации технических средств, а также при выводе технических средств или их элементов из эксплуатации, в том числе при передаче в ремонт.

5.Обязанности администратора информационной безопасности

На администратора информационной безопасности возлагаются обязанности по разработке и поддержанию в актуальном состоянии матрицы доступа к защищаемым информационным (программным) ресурсам КГКОУ Школа 4, включающей в себя:

▪перечень ИСПДн КГКОУ Школа 4;

▪перечень защищаемых информационных (программных) ресурсов КГКОУ Школа 4;

▪перечень сотрудников КГКОУ ШКОЛА 4, допущенных к самостоятельной работе на рабочих местах ИСПДн;

▪перечень сторонних лиц, имеющих доступ к ИСПДн КГКОУ Школа 4 в целях обработки ПДн;

▪перечень лиц, допущенных к обслуживанию ИСПДн КГКОУ Школа 4;

▪права различных категорий лиц, допущенных к работе на рабочих местах ИСПДн, в отношении защищаемых информационных (программных) ресурсов.

На основании матрицы доступа администратор информационной безопасности поручает администратору ИСПДн (системному администратору) создавать учетные записи пользователей ИСПДн и назначать им соответствующие права в отношении защищаемых ресурсов, генерировать необходимую для доступа к ИСПДн аутентификационную (парольную) и ключевую информацию, подготавливать при необходимости материальные носители аутентификационной и ключевой информации.

Администратор информационной безопасности по мере необходимости проводит инструктаж работников КГКОУ Школа 4 вопросам обеспечения безопасности ПДн, обрабатываемых в ИСПДн, при предоставлении им возможности доступа к ИСПДн и выдает под роспись пользователям ИСПДн материальные носители аутентификационной и ключевой информации (в случае их использования).

Администратору информационной безопасности запрещается разрешать доступ к ПДн, обрабатываемым в ИСПДн, работникам КГКОУ Школа 4, не включенным в перечень лиц, доступ к ПДн которым необходим для выполнения служебных (трудовых) обязанностей.

Администратор информационной безопасности несет ответственность за назначение лицам минимально необходимого им для выполнения служебных обязанностей набора прав в отношении защищаемых информационных (программных) ресурсов.

Длина паролей, выбираемых администратором информационной безопасности, должна быть не менее 12 символов. В качестве пароля должна быть выбрана последовательность букв верхнего и нижнего регистра с обязательным включением цифр и (или) специальных символов. Категорически запрещается использование в качестве пароля легко угадываемых последовательностей символов (идентификатор пользователя, его фамилия, имя или отчество, номер телефона, имена родственников, последовательно расположенные на стандартной клавиатуре символы, табельный номер и т. п.). Запрещается использование в качестве паролей слов распространенных мировых языков независимо от раскладки клавиатуры, в которой они набираются. Рекомендуется наряду с английскими буквами использовать буквы русского алфавита (с переключением набора символов на клавиатуре).

Пароли администратора информационной безопасности должны быть уникальными и не должны совпадать с другими паролями администратора информационной безопасности, в частности, с паролями электронной почты, программ обмена мгновенными сообщениями и др.

Максимальный срок использования паролей администратора информационной безопасности – 4 месяца.

Администратору информационной безопасности запрещается хранить пароли в записанном виде. За нарушение данного правила администратор информационной безопасности может быть привлечен к дисциплинарной ответственности.

Хранение администратором информационной безопасности паролей на бумажном носителе допускается только в личном, опечатанном

владельцем пароля сейфе, либо в сейфе директора КГКОУ ШКОЛА 4в опечатанном личной печатью пенале (конверте). При нарушении целостности печати или утрате бумажного носителя пароли считаются скомпрометированными и подлежат немедленной смене.

На администратора информационной безопасности возлагаются обязанности по разработке модели угроз безопасности ПДн, обрабатываемых в ИСПДн КГКОУ ШКОЛА 4, в соответствии с требованиями действующих нормативно-методических документов. Разрабатываемая администратором информационной безопасность модель угроз безопасности ПДн, обрабатываемых в ИСПДн, должна включать:

- описание возможных источников угроз безопасности ПДн, обрабатываемых в ИСПДн;
- оценку возможности реализации угроз безопасности ПДн с учетом принятых в КГКОУ ШКОЛА 4 мер защиты, условий функционирования ИСПДн, других объективных и субъективных факторов;
- оценку вреда, который может быть причинен субъекту ПДн в случае реализации угрозы безопасности ПДн.

Администратор информационной безопасности ежегодно осуществляет пересмотр (актуализацию) модели угроз безопасности ПДн, обрабатываемых в ИСПДн. Кроме того, актуализация модели угроз безопасности ПДн должна осуществляться в случае:

- ввода в эксплуатацию новой ИСПДн;
- внесения существенных изменений в технологический процесс обработки ПДн в ИСПДн КГКОУ ШКОЛА 4, в условия функционирования ИСПДн;
- реализации мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн, существенно влияющих на оценку возможности реализации угроз безопасности ПДн, обрабатываемых в ИСПДн.

Администратор информационной безопасности ведет учет применяемых средств защиты информации, эксплуатационной и технической документации к ним по установленной форме.

Администратор информационной безопасности обязан обеспечить надежное хранение дистрибутивов к средствам защиты информации, документации к ним, документации на СЗПДн в целом.

Администратор информационной безопасности регулярно проводит контроль соблюдения условий эксплуатации средств защиты информации, предусмотренных эксплуатационной и технической документацией.

Нарушение условий эксплуатации средств защиты информации является инцидентом информационной безопасности.

Администратор информационной безопасности организует доступ сторонних лиц к ИСПДн и (или) ее элементам при проведении работ по созданию, модернизации, эксплуатации СЗПДн, при сопровождении ИСПДн, обслуживании технических средств, способом, исключающим возможность несанкционированного доступа к ПДн или их носителям, в том числе, возможность хищения носителя ПДн. В случае невозможности исключения доступа к ПДн администратор информационной безопасности обязан под роспись уведомить сторонних лиц, получающих до- ступ к ИСПДн и (или) ее элементам о необходимости обеспечивать конфиденциальность (целостность, доступность) ПДн и ответственности за правонарушения в сфере информационной безопасности в соответствии с действующим законодательством.

Работы по созданию, модернизации, эксплуатации СЗПДн, обслуживанию технических средств проводятся сторонними лицами в присутствии администратора информационной безопасности. Работы по обслуживанию ИСПДн могут проводиться в присутствии лица, ответственного за эксплуатацию ИСПДн (по решению администратора информационной безопасности).

Администратор информационной безопасности контролирует размещение всех технических средств, участвующих в обработке ПДн, а также входящих в состав вычислительной сети КГКОУ ШКОЛА 4 (в случае, если технические средства ИСПДн так же входят в состав вычислительной сети), в том числе, сетевого оборудования, в пределах защищаемых помещений (защищаемых зданий, частей здания), исключение возможности несанкционированного доступа к техническим средствам, расположенным вне контролируемой зоны.

При выводе из эксплуатации (либо передаче сторонним организациям в целях ремонта) отдельных элементов ИСПДн администратор информационной безопасности обязан обеспечить удаление из запоминающих устройств ПДн и технологической (служебной, конфигурационной, управляющей и т. д.) информации способом, предусмотренным технологией записи в запоминающее устройство.

Если пользователь сообщает о невозможности входа в систему под своей учетной записью, администратор информационной безопасности должен:

- убедиться в том, что сотрудник правильно вводит имя пользователя;

▪убедиться в том, что учетная запись не заблокирована;

▪проанализировать содержимое журналов безопасности с целью выявления успешных и неуспешных попыток входа в систему с использованием данной учетной записи и узлов сети, с которых осуществлялся вход;

▪сопоставить данные, полученные в результате анализа журналов безопасности, с информацией о режиме работы данного пользователя и его личной рабочей станции;

▪установить причины нештатной ситуации и определить, имел ли место инцидент информационной безопасности;

▪в случае если событие не отнесено к категории инцидентов информационной безопасности, устранить причины нештатной ситуации и обеспечить возможность входа пользователя в систему;

▪в случае инцидента информационной безопасности осуществить процедуру реагирования на инцидент информационной безопасности в порядке, описанном в настоящей Инструкции.

При возникновении подозрения о компрометации пароля администратор информационной безопасности должен:

▪обеспечить незамедлительную смену скомпрометированного пароля (или убедиться, что смена пароля уже произведена пользователем);

▪установить время и дату предполагаемой компрометации пароля;

▪проанализировать содержимое журналов безопасности начиная со дня, предшествующего предполагаемой дате компрометации, с целью обнаружения фактов входа в систему с использованием учетной записи пользователя, чей пароль был скомпрометирован, и узлов сети, с которых осуществлялся вход;

▪сопоставить данные, полученные в результате анализа журналов безопасности, с информацией о режиме работы пользователя, использующего данную учетную запись, и его личной рабочей станции;

▪установить, имел ли место инцидент информационной безопасности;

▪в случае инцидента информационной безопасности осуществить процедуру реагирования на инцидент информационной безопасности в порядке, описанном в настоящей Инструкции.

При поступлении сообщения о возникновении нештатной ситуации (события, выходящего за рамки штатного функционирования КГКОУ Школа 4) администратор информационной безопасности совместно с системным администратором осуществляет оперативный сбор информации, связанной с событием, и оценку этой информации с целью определения, относится ли событие к категории инцидентов информационной безопасности. К инцидентам информационной безопасности должны быть отнесены следующие события:

▪уничтожение или блокирование данных, технических средств, инфраструктуры и элементов ИСПДн вследствие стихийного бедствия, пожара, затопления или техногенных факторов (сбои, отказы программного обеспечения, технических средств, систем обеспечения функционирования ИСПДн);

▪нежелательная сетевая активность (сканирование сети, попытки подбора пароля, взлома системы защиты или воздействия на технические (в том числе, программные) средства);

▪уничтожение, кража носителей ПДн, раскрытие, модификация или блокирование ПДн вследствие несанкционированного проникновения в контролируемую зону;

▪утрата отчуждаемого носителя информации;

▪уничтожение, модификация, блокирование, раскрытие информации или нарушение работоспособности ИСПДн вследствие успешно проведенной атаки или воздействия вредоносного программного обеспечения;

▪уничтожение, модификация, блокирование, раскрытие информации или нарушение работоспособности ИСПДн, совершенные пользователем ИСПДн (или от его имени) с использованием назначенных ему прав;

▪нарушение установленных в КГКОУ ШКОЛА 4 требований по безопасности.

При отнесении события к категории инцидентов информационной безопасности, администратор информационной безопасности совместно с системным администратором должен оценить уровень потенциального риска (путем определения возможности и характера ущерба, оценки темпа развития инцидента информационной безопасности):

уровень 1 – инцидент информационной безопасности является локальным и может быть разрешен силами КГКОУ ШКОЛА 4;

уровень 2 – инцидент информационной безопасности может привести к существенному ущербу и может быть разрешен силами КГКОУ Школа 4 лишь частично;

уровень 3 – последствия инцидента информационной безопасности являются критическими, и он не может быть разрешен силами КГКОУ Школа 4.

В случае отнесения инцидента информационной безопасности к уровню 2 или уровню 3 незамедлительно уведомляется лицо, ответственное за организацию обработки ПДн, и КГКОУ ШКОЛА 4.

Администратор информационной безопасности совместно с системным администратором (с привлечением при необходимости иных сотрудников и специалистов) осуществляют локализацию инцидента информационной безопасности. При локализации инцидента информационной безопасности указанные сотрудники с учетом оценки реальной ситуации и существующих возможностей под свою ответственность осуществляют выбор стратегии и способа реагирования на инцидент информационной безопасности. В рамках локализации инцидента информационной безопасности могут быть предприняты реактивные действия (отключение технических средств от внешних сетей или их изоляция; изменение настроек межсетевого экрана, маршрутизаторов, других технических средств; принятие иных экстренных мер) или проактивные действия (наблюдение, предупреждение дальнейшего развития инцидента информационной безопасности)). Допустимость реактивных действий определяется с учетом характера инцидента информационной безопасности и уровня потенциального риска в случае непринятия реактивных мер.

После локализации инцидента информационной безопасности администратором информационной безопасности составляется письменный отчет об инциденте информационной безопасности, его копия направляется лицу, ответственному за организацию обработки ПДн, и директору КГКОУ ШКОЛА 4. На администратора информационной безопасности возлагается ответственность за достоверность сведений,

указанных в отчете об инциденте информационной безопасности. В отчете должны быть зафиксированы:

▪дата и время, когда произошел инцидент информационной безопасности;

▪перечень лиц (должность, фамилия, имя, отчество), бывших свидетелями события или сообщивших о нем;

▪описание инцидента информационной безопасности;

▪перечень свидетельств события и место их хранения (при наличии свидетельств);

▪последовательность проведенных мероприятий и действий по локализации инцидента информационной безопасности, описание использованных при этом средств;

▪описание ущерба и иных последствий инцидента информационной без- опасности, в том числе вероятных последствий;

▪выводы о возможных причинах инцидента информационной безопасности. Данный документ хранится у администратора информационной безопасности.

Администратор информационной безопасности отвечает за обеспечение сохранности информации, относящейся к инциденту информационной безопасности. Указанная информация в дальнейшем может использоваться при проведении компьютерно-технической экспертизы, а также в качестве доказательной базы при судебном разбирательстве.

Администратору информационной безопасности запрещается:

без согласования со специализированной организацией, осуществляющей сопровождение СЗПДн, изменять состав используемых на рабочих местах и серверах ИСПДн программных средств (в том числе, деинсталлировать установленные средства защиты информации; удалять или менять версию антивирусной программы; устанавливать программы, не участвующие в технологическом процессе обработки информации);

▪изменять настройки средств защиты информации без согласования со специализированной организацией, осуществляющей сопровождение СЗПДн;

▪использовать любые USB-устройства, не участвующие в технологическом процессе обработки информации и не зарегистрированные в соответствующем журнале;

▪передавать сторонним организациям в целях ремонта носители

информации, которые могут содержать ПДн (жесткие диски, USB-носители и т. п.);

▪использовать предоставленные полномочия в целях, отличных от целей, предусмотренных служебными обязанностями;

▪производить в рабочее время действия, приводящие к сбою, остановке, замедлению работы автоматизированной системы (ИСПДн), блокировке, потере информации, без предупреждения пользователей.

Права администратора информационной безопасности

Администратор информационной безопасности имеет право:

▪осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности с последующим докладом лицу, ответственному за организацию обработки ПДн, и главному врачу КГКОУ ШКОЛА 4;

▪вносить свои предложения по совершенствованию мер защиты обрабатываемых ПДн.

Краевое государственное казенное общеобразовательное учреждение,
реализующее адаптированные основные общеобразовательные программы
«Школа № 4»

Приложение 4

УТВЕРЖДЕНО
приказом директора школы
от 28.01.2022. № 20\1Д

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах персональных данных

г. Амурск
2022 год

1. **Общие положения**

1.1. Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаление учетных записей пользователей) в информационной системе персональных (далее – ИСПДн) в Краевом государственном казенном общеобразовательном учреждении, реализующим адаптированные основные общеобразовательные программы "школа № 4" (далее – КГКОУ Школа 4).

1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник КГКОУ Школа 4, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации ИСПДн (далее – СЗИ).

1.4. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн и контроль над действиями Пользователей в ИСПДн осуществляет ответственный за обеспечение безопасности персональных данных в КГКОУ Школа 4 (далее – Ответственный).

1.5. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) Пользователей осуществляет администратор ИСПДн в КГКОУ Школа 4 (далее – Администратор).

2. **Организация парольной защиты**

2.1. Личные пароли должны создаваться Пользователями самостоятельно.

2.2. В случае формирования личных паролей Пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного и Администратора в ИСПДн и на АРМ Пользователей соответственно.

2.3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 4 месяца.

2.4. Внеплановая смена личного пароля Пользователя или удаление учетной записи в случае прекращения его полномочий

(увольнение, переход на другую должность в ИСПДн и т.п.) должна производиться Администратором и Ответственным немедленно после окончания последнего сеанса работы Пользователя в АРМ и в ИСПДн соответственно.

2.5. В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) Пользователя, равное 7, после чего учетная запись блокируется.

2.6. Разблокирование учетной записи осуществляется Администратором и Ответственный для учетных записей Пользователя для АРМ и для ИСПДн соответственно.

3. **Требования к формированию паролей**

Пользователи при формировании паролей должны руководствоваться следующими требованиями:

3.1. Длина пароля должна быть не менее 6 символов.

3.2. В пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих:

- буквы в верхнем регистре;
- буквы в и нижнем регистре;
- цифры;

3.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.).

3.4. Пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть.

3.5. Пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе.

3.6. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.).

3.7. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

4. **Правила ввода паролей**

Пользователи во время процедуры аутентификации (ввода логина и пароля) на АРМ и в ИСПДн должны руководствоваться следующими правилами:

4.1. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

4.2. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и пр.).

4.3. В случае блокировки учетной записи Пользователя после превышения попыток ввода данных аутентификации (логина и пароля) в АРМ или ИСПДн, Пользователю необходимо уведомить Администратора или Ответственный соответственно для проведения процедуры генерации нового пароля.

5. **Обязанности**

Пользователи ИСПДн обязаны:

5.1. Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов КГКОУ Школа 4 по парольной защите.

5.2. Своевременно сообщать Ответственному и Администратору об утере, компрометации и несанкционированном изменении сроков действия паролей в АРМ и ИСПДн соответственно.

5.3. Ознакомиться под роспись с перечисленными в настоящей инструкции требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

6. **Ответственность**

6.1. Пользователь несет персональную ответственность за сохранность данных аутентификации (персонального логина и пароля) к АРМ и к ИСПДн.

Краевое государственное казенное общеобразовательное учреждение, реализующее адаптированные основные общеобразовательные программы
«Школа № 4»

Приложение 5

УТВЕРЖДЕНО
приказом директора школы
от 28.01.2022. № 20\1Д

ИНСТРУКЦИЯ
по организации антивирусной защиты

г. Амурск
2022 год

1. Общие положения

1.1. Настоящая инструкция разработана в целях защиты персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн) в краевом государственном казенном общеобразовательном учреждении, реализующим адаптированные основные общеобразовательные программы "школа № 4" (далее – КГКОУ Школа 4) от несанкционированного копирования, модификации и уничтожения под действием вирусов и другого вредоносного программного обеспечения (далее – ПО).

1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник КГКОУ Школа 4, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации ИСПДн (далее – СЗИ).

1.4. Организация антивирусной защиты в ИСПДн при обработке ПДн Пользователями в ИСПДн осуществляется ответственный за обеспечение безопасности персональных данных в КГКОУ Школа 4.

1.5. Контроль над работой Пользователя по применению на автоматизированных рабочих местах (далее – АРМ) ИСПДн антивирусной защиты осуществляет ответственный за обеспечение безопасности персональных данных информационной системы персональных данных в КГКОУ Школа 4.

2. Организация антивирусной защиты

2.1. К применению на АРМ и серверах ИСПДн допускается только лицензионные и сертифицированные ФСТЭК России антивирусные средства.

2.2. К настройке системы антивирусной защиты допускаются только, уполномоченные сотрудники, утвержденные руководством КГКОУ Школа 4.

2.3. Пользователям запрещено вмешиваться в работу системы антивирусной защиты.

2.4. Обо всех неисправностях или неполадках пользователь обязан сообщить ответственному за обеспечение безопасности

персональных данных информационных систем персональных данных КГКОУ Школа 4.

2.5. На АРМ ИСПДн запрещается установка ПО, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

2.6. Пользователь при работе со съёмными носителями информации обязан перед началом работы провести их проверку средствами антивирусной защиты на предмет отсутствия компьютерных вирусов и вредоносных программ.

2.7. Все факты модификации и разрушения данных на серверах или АРМ ИСПДн, а также заражение их вирусами или вредоносным ПО, должны анализироваться ответственным за обеспечение безопасности персональных данных в КГКОУ Школа 4.

2.8. Ответственный за обеспечение безопасности персональных данных в КГКОУ Школа 4 осуществляет полную проверку жесткого диска АРМ и северов ИСПДн и съемных носителей на наличие вирусов и вредоносного ПО не реже 1 раза в месяц.

2.19. Антивирусное ПО должно запускаться автоматически при старте операционной системы АРМ и серверов ИСПДн и функционировать до завершения работы операционной системы.

2.10. На АРМ и серверах ИСПДн должно быть предусмотрен запрет пользователям на блокировку и выгрузку антивирусного ПО.

3. Действия при обнаружении вирусов

3.1. Пользователи при обнаружении или появления подозрений на наличие компьютерных вирусов или вредоносного ПО обязаны немедленно прекратить какие-либо действия на АРМ ИСПДн и провести лечение зараженных файлов путем выбора соответствующего пункта меню антивирусной программы и затем провести повторный антивирусный контроль.

3.2. В случае обнаружения на съёмных носителях информации нового вируса или вредоносного ПО, не поддающегося лечению, пользователь обязан прекратить их использование.

3.3. В случае обнаружения на АРМ ИСПДн не поддающегося лечению вируса или вредоносного ПО, Пользователь обязан поставить в известность ответственного за обеспечение безопасности персональных данных в КГКОУ Школа 4 и, прекратить работу на АРМ и в возможно короткие сроки принять необходимые меры к устранению вируса (обновить пакет антивирусных программ и т.п.).

4. **Ответственность**

4.1. Пользователь несет персональную ответственность за осуществление регламента использования на АРМ ИСПДн антивирусных средств.