Приложение 6/1
к приказу МКОУ «Липковская СОШ № 2»
от 02.09.2024 № 118/1

ИНСТРУКЦИЯ
ПО УЧЕТУ ЛИЦ, ДОПУЩЕННЫХ К РАБОТЕ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ
В МКОУ «ЛипковскаяСОШ № 2»

1. Настоящая инструкция по учету лиц, допущенных к работе с персональными данными в МКОУ «Липковская СОШ № 2»), разработана в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119; Требованиями Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687.
2. Инструкция определяет порядок учета лиц, допущенных к работе с персональными данными обрабатываемых в информационных системах в МКОУ «ЛипковскаяСОШ № 2».
3. Основанием для допуска сотрудника к работе с персональными данными является:
- включение в список допущенных сотрудников к работе с персональными данными в ОУ на основании приказа директора;
- прохождение первичного инструктажа, включая ознакомление со всеми нормативными документами, регламентирующими работу с персональными данными;
- определение перечня информационных систем, необходимых для выполнения своих должностных обязанностей;
- внесение соответствующих данных в Журнал учёта прохождения первичного инструктажа сотрудниками, допущенными к работе с персональными данными.
4. Основанием для прекращения допуска сотрудников к персональным данным является:
- прекращение трудовых отношений;
- изменение его должностных обязанностей;
- обнаружение нарушений порядка обработки персональных данных;
- обнаружение нарушений порядка обработки персональных данных до выяснения и устранения причин нарушений.
5. Лица, допущенных к работе с персональными данными, несут персональную ответственность: - за сохранность сведений ограниченного распространения в соответствии с требованиями законодательства в области защиты персональных данных;
- за качество и полноту проводимых им работ по организации обработки персональных данных;
- за правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

С инструкцией ознакомлен (а), экземпляр инструкции получил(а)

«___»_____20___ г. _____/_____/

Приложение 6/2
к приказу МКОУ «Липковская СОШ № 2»
от 02.09.2024 № 118/1

ИНСТРУКЦИЯ
по проведению инструктажа лиц,
допущенных к работе с информационной системой персональных данных МКОУ «Липковская СОШ № 2»

1. Настоящая инструкция разработана с целью обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных МКОУ «Липковская СОШ № 2» (далее – ИСПДн).

2. При поступлении на работу сотрудника, которому для выполнения своих трудовых обязанностей необходим доступ к ИСПДн (далее – новый сотрудник), ответственный за организацию обработки персональных данных:

– в соответствии с п.6 ч.1 ст.18.1 Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных» проводит ознакомление нового сотрудника с положениями законодательства Российской Федерации о персональных данных и правовыми актами МКОУ «Липковская СОШ № 2» в отношении обработки персональных данных, перечисленными в Приложении № 1 к данной инструкции;

– знакомит нового сотрудника с ответственностью за неисполнение требований по обеспечению безопасности персональных данных в ИСПДн, предусмотренной действующим законодательством Российской Федерации;

– отмечает в Журнале учета прохождения первичного инструктажа данные о проведении инструктажа.

3. Новый сотрудник может приступить к исполнению своих непосредственных трудовых обязанностей, связанных с обработкой персональных данных, только после успешного прохождения первичного инструктажа.

С Инструкцией ознакомлены:

_____	_____	_____
дата	подпись	ФИО

Приложение 1 к Инструкции по проведению инструктажа лиц, допущенных к работе с информационными системами персональных данных

Перечень законодательных актов Российской Федерации о персональных данных, документов, определяющих требования к защите персональных данных, внутренних локальных актов, определяющих политику организации в отношении обработки персональных данных, с которыми необходимо ознакомить нового сотрудника при проведении первичного инструктажа

Законодательные акты Российской Федерации о персональных данных:

1) Федеральный закон от 27.07.2006 г. N 149-ФЗ "О информации, информационных технологиях и о защите информации"
2) Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 21.07.2014).
3) Федеральный закон от 2 марта 2007 г. N 25-ФЗ "О муниципальной службе в Российской Федерации"
4) Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (для сотрудников, обрабатывающих персональные данные в том числе без использования средств автоматизации).
5) Постановление Правительства Российской Федерации от 21 марта 2012 года N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"
6) Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
7) Приказ о допуске к обработке персональных данных.
8) Политика в отношении обработки персональных данных.
9) Положение об обработке персональных данных.
10) Положение о порядке доступа в помещения, в которых ведётся обработка персональных данных.
11) Положение об обработке персональных данных без использования средств автоматизации.
12) Инструкция по учёту и хранению съёмных носителей персональных данных
13) Инструкция по организации резервного копирования и восстановления в ИСПДн.
14) Инструкция по учёту лиц, допущенных к обработке.
15) Инструкция по антивирусной защите.
16) Инструкция по проведению инструктажа лиц, допущенных к работе с ПДн.
17) Правила осуществления внутреннего контроля.
18) Инструкция по порядку уничтожения и обезличивания персональных данных.
19) Инструкция пользователя ИСПДн.
20) Инструкция пользователя при возникновении нештатной ситуации.
21) План проведения внутреннего контроля.
22) Приказ об утверждении перечня помещений, в которых ведется обработка.

Приложение № 6/3
к приказу МКОУ «Липковская СОШ № 2»
от 02.09.2024 № 118/1

ИНСТРУКЦИЯ
по работе пользователей ИСПДн

1. Общие положения

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

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

Пользователь несет персональную ответственность за свои действия.

Пользователь в своей работе руководствуется настоящей инструкцией, и нормативными документами школы.

Методическое руководство работой пользователя осуществляется ответственным за организацию обработки персональных данных.

2. Должностные обязанности

Пользователь обязан:

- 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.
- Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении об организации работы с персональными данными в ОУ.
- 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.
- Соблюдать требования инструкции по организации парольной защиты.
- Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет.

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).

Обо всех выявленных нарушениях, связанных с информационной безопасностью школы, а также для получений консультаций по вопросам информационной безопасности, необходимо обращаться к Администратору ИСПДн (или ответственному за организацию обработки персональных данных).

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

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;
- несанкционированноотрыватьобщийдоступкпапкамнасвоейрабочейстанции;
- 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 настройкиАРМ,без согласования с ответственным за обработку персональных данных.

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>.

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

3. Правила работы в сетях общего доступа и(или) международного обмена

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

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 с потенциально опасным содержимым (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

4. Права и ответственность пользователей ИСПДн

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

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.

С Инструкцией ознакомлены:

_____	_____	_____
ФИО	Подпись	Дата
_____	_____	_____

Приложение 6/4
к приказу МКОУ «Липковская СОШ № 2»
от 02.09.24 № 118/1

Инструкция по учету и хранению съемных носителей персональных данных в МКОУ «Липковская СОШ № 2»

1. Общие положения

1.1. Настоящая инструкция по учету и хранению съемных носителей персональных данных в МКОУ «Липковская СОШ № 2» (далее — Инструкция) определяет порядок работы со съемными носителями персональных данных в МКОУ «Липковская СОШ № 2» (далее – Школа) в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Инструкция подлежит к выполнению всеми сотрудниками Школы, допущенными к обработке персональных данных в соответствии с Перечнем должностей МКОУ «Липковская СОШ № 2», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

2. Определения

2.1. Съемный носитель персональных данных – носитель информации, используемый для хранения и передачи персональных данных в электронной форме.

2.2. Пользователь – штатный сотрудник Школы или сотрудник по договору гражданско-правового характера, допущенный к обработке персональных данных в МКОУ «Липковская СОШ № 2» и указанный в Перечне должностей в МКОУ «Липковская СОШ № 2», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

3. Порядок работы со съемными носителями

3.1. Ответственный за безопасность информационных систем персональных данных Школы, назначенный приказом МКОУ «Липковская СОШ № 2», выдает съемные носители Пользователям только в случаях служебной необходимости.

3.2. Все съемные носители персональных данных учитываются в Журнале учета съемных носителей, содержащих персональные данные и выдаются Пользователям под подпись.

3.3. Пользователям, получившим съемные носители персональных данных под подпись, запрещается передавать их третьим лицам.

3.4. Ответственный за безопасность изымает съемные носители персональных данных при увольнении Пользователя.

3.5. Все съемные носители персональных данных хранятся в запираемых шкафах или сейфах (металлических шкафах) с кодовыми или внутренними замками (с не менее чем двумя дубликатами ключей).

3.6. Допускается хранение съемных носителей персональных данных вне запираемых шкафов или сейфов (металлических шкафов) при условиях уничтожения персональных данных, либо если на съемном носителе персональных данных хранятся только персональные данные в зашифрованном или обезличенном виде.

3.7. Право на перемещение съемных носителей информации за пределы территории (контролируемой зоны, определенной Положением об определении границ контролируемой зоны на которой осуществляется обработка, имеют только те сотрудники Школы, которым это необходимо для выполнения своих должностных обязанностей.

3.8. Использование неучтенных съемных носителей для обработки персональных данных фиксируется как несанкционированное, а Ответственный за безопасность инициирует служебную проверку. По факту выясненных обстоятельств составляется Акт проведения внутреннего расследования по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных

3.9. Пользователи, в случаях утраты или кражи съемных носителей персональных данных, сообщают об этом Ответственному за безопасность.

3.10. Съемные носители персональных данных, пришедшие в негодность, или отслужившие в установленный срок, подлежат уничтожению. По результатам уничтожения составляется Акт уничтожения носителей, содержащих персональные данные субъектов.

4. Порядок организации учета съемных носителей

4.1. На каждом съемном носителе персональных данных размещается этикетка с уникальным учетным номером.

4.2. Ответственный за безопасность при выдаче, приеме, уничтожении съемных носителей персональных данных вносит информацию о съемном носителе в Журнале учета съемных носителей, содержащих персональные данные.

4.3. Пользователи при получении либо сдаче съемных носителей персональных данных заносят в Журнал учета съемных носителей, содержащих персональные данные, свои фамилию, имя, отчество, ставят дату и подпись.

5. Ответственность

5.1. Все сотрудники Школы, допущенные в установленном порядке к работе с персональными данными и указанные в Перечне должностей МКОУ «Липковская СОШ № 2», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством за обеспечение сохранности и соблюдению правил работы с персональными данными.

5.2. Ответственность за доведение требований настоящей Инструкции до сотрудников Школы несет ответственный сотрудник за проведение инструктажа лиц, допущенных к работе с персональными данными в Школе, назначенный настоящим распоряжением.

5.3. Ответственность за обеспечение мероприятий по реализации требований настоящей Инструкции, в том числе учет, выдачу, уничтожение съемных носителей персональных данных несет Ответственный за безопасность.

С Инструкцией ознакомлены:

_____	_____	_____
дата	подпись	ФИО

Приложение 6/5
к приказу МКОУ «Липковская СОШ № 2»
от 02.09.24 № 118/1

ИНСТРУКЦИЯ
по организации антивирусной защиты информационных систем персональных данных МКОУ «Липковская СОШ № 2»

Настоящая инструкция определяет порядок организации антивирусной защиты на информационных системах персональных данных МКОУ «Липковская СОШ № 2» (далее - ИСПДн).

1. Общие положения

1.1. Настоящая Инструкция предназначена для администратора ИБ ИСПДн, ответственного за ЗИ на объекте информатизации и пользователей, эксплуатирующих ИСПДн МКОУ «Липковская СОШ № 2».

1.2. Инструкция устанавливает требования и ответственность при организации защиты информации, в ИСПДн от программно-математических воздействий и разрушающего воздействия компьютерных вирусов.

1.3. В целях закрепления знаний по вопросам практического исполнения требований Инструкции, разъяснения возникающих вопросов, проводятся организуемые Администратором ИБ ИСПДн семинары и персональные инструктажи (при необходимости) пользователей ИСПДн.

1.4. Инструкция регулирует как вопросы организации антивирусной защиты, так и требования к порядку проведения антивирусного контроля при работе в ИСПДн.

2. Применение средств антивирусной защиты

1.5. Антивирусный контроль дисков и файлов ИСПДн после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

1.6. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн (сканирование).

1.7. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

1.8. Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с «Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных МКОУ «Липковская СОШ № 2».

1.9. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

3. Функции Администратора ИСПДн по обеспечению антивирусной безопасности

Администратор ИБ ИСПДн обязан:

3.1. При необходимости проводить инструктажи пользователей ИСПДн по вопросам применения средств антивирусной защиты.

3.2. Настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.

3.3. Предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов.

3.4. При необходимости производить обновление антивирусных программных средств.

3.5. Производить получение и рассылку (при необходимости) обновлений антивирусных баз.

3.6. При необходимости разрабатывать инструкции по работе пользователей с программными средствами САЗ.

3.7. Проводить работы по обнаружению и обезвреживанию вирусов.

3.8. Участвовать в работе комиссии по расследованию причин заражения ПК и серверов.

3.9. Хранить эталонные копии антивирусных программных средств.

3.10. Осуществлять периодический контроль за соблюдением пользователями ПК требований настоящей Инструкции;

3.11. Разрабатывать инструкции по работе пользователей с системой антивирусной защиты информации.

3.12. Проводить периодический контроль работы программных средств системы антивирусной защиты информации на ПК (серверах).

4. **Функции пользователей**

Пользователи ИСПДн получают по ЛВС или от Администратора ИБ ИСПДн носители с обновлениями антивирусных баз (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.1. Проводят обновления антивирусных баз на ПК (в случае отсутствия механизмов централизованного распространения антивирусных баз).

4.2. 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 подразделения самостоятельно или вместе с администратором ИБ ИСПДн должен провести внеочередной антивирусный контроль ПК. При необходимости он должен пригласить Администратора ИБ ИСПДн для определения факта наличия или отсутствия компьютерного вируса.

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

4.3.1. приостановить работу;

4.3.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения и Администратора ИБ ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

4.3.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

4.3.4. провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта пригласить Администратора ИБ ИСПДн);

4.3.5. в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, передать зараженный вирусом файл на съемном носителе Администратору ИБ ИСПДн для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку;

4.3.6. по факту обнаружения зараженных вирусом файлов составить служебную записку Администратору ИБ ИСПДн, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

5. **Ответственность при организации антивирусной защиты**

5.1.1. Ответственность за организацию антивирусной защиты ИСПДн и установление порядка ее проведения, в соответствии с требованиями настоящей Инструкции, возлагается на ответственного за ЗИ в ИСПДн.

5.1.2. Ответственность за поддержание установленного порядка и соблюдение требований настоящей Инструкции возлагается на Администратора ИБ в ИСПДн и пользователей (операторов).

5.1.3. Периодический контроль за выполнением всех требований настоящей Инструкции, и состоянием антивирусной защиты осуществляется Администратором ИБ ИСПДн.

С Инструкцией ознакомлены:

_____	_____	_____
дата	подпись	ФИО

Приложение 6/6
к приказу МКОУ «Липковская СОШ № 2»
от 02.09.2024г. № 118/1

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных при возникновении нештатных ситуаций МКОУ «Липковская СОШ № 2»

1. Общие положения

Настоящая инструкция пользователя информационных систем персональных данных МКОУ «Липковская СОШ № 2» при возникновении нештатных ситуаций (далее – Инструкция) определяет возможные аварийные ситуации, связанные с функционированием информационных систем персональных данных (далее – ИСПДн) МКОУ «Липковская СОШ № 2» (далее – Администрация), указанных в Перечне информационных систем персональных данных МКОУ «Липковская СОШ № 2»; меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после аварийных ситуаций.

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

Задачами настоящей Инструкции являются:

- определение мер защиты от прерывания работоспособности;
- определение действий по восстановлению в случае прерывания работоспособности.

Действие настоящей Инструкции распространяется на всех пользователей ИСПДн школы (далее – Пользователи), 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.

Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из следующих угроз:

Технологические угрозы:

- пожар в здании;
- повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения);
- взрыв (бытового газа, взрывчатых веществ или приборов, работающих под давлением);
- химический выброс в атмосферу.

Внешние угрозы:

- массовые беспорядки;
- сбои общественного транспорта;
- эпидемия;
- массовое отравление персонала;
- теракт.

Стихийные бедствия:

- удар молнии;

- сильный снегопад;
- сильные морозы;
- просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания;
- затопление водой в период паводка;
- наводнение, вызванное проливным дождем;
- торнадо;
- подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).

Угрозы в сфере информационных технологий:

- сбой системы кондиционирования в серверном помещении;
- выход из строя файлового сервера;
- частичная потеря информации на сервере без потери его работоспособности;
- выход из строя локальной сети;
- выход из строя рабочей станции;
- частичная потеря информации на рабочей станции без потери её работоспособности.

Угроза, связанная с человеческим фактором:

- ошибка персонала, имеющего доступ к элементам ИСПДн;
- нарушение конфиденциальности, целостности и доступности конфиденциальной информации, а также несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Угрозы, связанные с внешними поставщиками:

- отключение электроэнергии;
- сбой в работе интернет-провайдера;
- физический разрыв внешних каналов связи.

2. Действия при возникновении нештатной ситуации

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

Уровень 1. Незначительный инцидент – локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты.

Уровень 2. Авария – любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты;

Уровень 3. Катастрофа – любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, к уничтожению, блокированию, неправомерной модификации или компрометации защищаемых персональных данных, а также к угрозе жизни Пользователей ИСПДн.

При возникновении нештатной ситуации любого уровня Пользователь обязан оповестить ответственное лицо за организацию обработки персональных данных МКОУ «Липковская СОШ № 2», назначенного приказом директора, сообщив характер аварийной ситуации, масштаб ситуации по предварительной субъективной оценке.

Все действия в процессе реагирования на аварийные ситуации должны документироваться администратором безопасности ИСПДн в Журнале регистрации фактов нарушения и восстановления работоспособности оборудования или информационных систем персональных данных МКОУ «Липковская СОШ № 2». В

кратчайшие сроки, не превышающие одного рабочего дня, должны быть предприняты меры по восстановлению работоспособности ИСПДн.

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

системы жизнеобеспечения:
пожарные сигнализации и системы пожаротушения;
системы вентиляции и кондиционирования;
системы резервного питания;
системы обеспечения отказоустойчивости;
системы резервного копирования и хранения данных;
системы контроля физического доступа.

Все критичные помещения, в которых размещаются элементы ИСПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения. Порядок предотвращения потерь информации и организации восстановления ИСПДн описан в Инструкции по организации резервирования и восстановления программного обеспечения, баз персональных данных информационных систем персональных данных администрации.

Ответственный сотрудник за проведение инструктажа лиц, допущенных к работе с персональными данными в МКОУ «Липковская СОШ № 2» назначенный настоящим распоряжением проводит следующие мероприятия:

ознакамливает всех сотрудников школы, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3х рабочих дней с момента выхода нового сотрудника на работу;

обучает сотрудников школы, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций.

Пользователи 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 руководителями структурных подразделений;
выключение оборудования, электричества, водоснабжения, газоснабжения.

Навыки и знания Пользователей по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение Пользователей порядку действий при возникновении аварийной ситуации. Ответственность за организацию обучения Пользователей несет ответственное лицо за организацию обработки персональных данных в МКОУ «Липковская СОШ № 2».

С Инструкцией ознакомлены:

_____	_____	_____
дата	подпись	ФИО

Приложение 6/7
к приказу МКОУ «Липковская СОШ № 2»
от 02.09.24 № 118/1

ИНСТРУКЦИЯ
по резервному копированию и восстановлению информационных ресурсов информационных систем персональных данных МКОУ «Липковская СОШ № 2»

Резервное копирование информации, хранящейся в информационной системе персональных данных (далее ИСПДн), настраивается и производится под контролем ответственного за обеспечение безопасности персональных данных однократно после подготовки ИСПДн к работе и хранится:

- одна копия–на локальном жестком диске;
- вторая копия–на отчуждаемом учтенном носителе.

1. Резервное копирование защищаемой информации (ПДн) производится еженедельно администратором безопасности ИСПДн.
2. После окончания процесса резервного копирования полученную резервную копию (архив) следует скопировать на отчуждаемый учтенный носитель.
3. При втором и последующих резервных копированиях текущего месяца возможно создание инкрементных архивов (если данная возможность предусмотрена в средствах резервного копирования).
4. В случае нехватки свободного дискового пространства для сохранения файла архива следует удалить наиболее старый архив.
5. На отчуждаемом носителе должны храниться архивы не менее чем за два месяца: текущий и предыдущий.
6. В случае необходимости восстановления данных из резервной копии, для восстановления следует использовать наиболее поздний архив. В случае невозможности использования наиболее позднего архива по каким-либо причинам, архив, используемый для восстановления, выбирается совместным решением администратора и ответственного за обеспечение безопасности персональных данных.

С Инструкцией ознакомлены:

_____	_____	_____
дата	подпись	ФИО

Приложение № 6/8
к приказу МКОУ «Липковская СОШ № 2»
от 02.09.24 № 118/1

ИНСТРУКЦИЯ
ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ
ПЕРСОНАЛЬНЫХ ДАННЫХ В МКОУ «ЛИПКОВСКАЯ СОШ № 2»

1. Общие положения

Настоящая Инструкция о лице, ответственном за обработку персональных данных, в МКОУ «Липковская СОШ № 2» (далее — Инструкция) определяет основные задачи, функции, права Ответственного за организацию обработки персональных данных (далее — ПДн) МКОУ «Липковская СОШ № 2». Настоящая Инструкция разработана во исполнение требований Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

Ответственный за организацию обработки ПДн является работником МКОУ «Липковская СОШ № 2» и назначается приказом директора МКОУ «Липковская СОШ № 2». В своей деятельности Ответственный за организацию обработки ПДн руководствуется законодательством Российской Федерации, настоящей Инструкцией и другими внутренними нормативными документами МКОУ «Липковская СОШ № 2».

2. Функции ответственного за организацию обработки ПДн

Основными функциями Ответственного за организацию обработки ПДн являются:

– обеспечение соблюдения требований законодательства Российской Федерации в части обработки ПДн, нормативных правовых актов, регулирующих обработку ПДн, а также внутренних организационно-распорядительных документов;

– обеспечение правомерности обработки персональных данных, а также соответствия процессов обработки ПДн заявленным целям;

– обеспечение соответствия договоров и соглашений, заключаемых с третьими лицами и связанных с передачей, совместной обработкой или поручением обработки персональных данных, требованиям законодательства Российской Федерации;

– мониторинг изменений законодательства Российской Федерации по вопросам обработки ПДн;

– разработка внутренних нормативных документов по организации обработки ПДн и контроль за их исполнением;

– организация мероприятий по повышению осведомленности работников ОУ по вопросам обработки ПДн;

– изучение и анализ вновь выходящих нормативно-правовых и методических документов в области обработки ПДн;

– организация и ведение учета лиц, допущенных к обработке ПДн в МКОУ «Липковская СОШ № 2».

3. Права и обязанности Ответственного за организацию обработки ПДн

Ответственный за организацию обработки ПДн имеет право:

– по согласованию с директором МКОУ «Липковская СОШ № 2» давать структурным подразделениям *наименование организации* и отдельным работникам обязательные для исполнения указания по вопросам, входящим в компетенцию Ответственного за организацию обработки ПДн;

– запрашивать и получать от структурных подразделений *наименование МКОУ «Липковская СОШ № 2»* сведения, справочные и другие материалы, необходимые для исполнения своих обязанностей всоответствии с настоящим Положением;

– инициировать проведение служебных расследований по фактам нарушения установленных правил обработки ПДн и обеспечения безопасности ПДн и предоставлять *директору МКОУ «Липковская СОШ № 2»* отчет о проведенных служебных расследованиях с представлением информации о субъектах доступа, нарушивших режим доступа;

– готовить предложения о привлечении к проведению работ по обеспечению безопасности ПДн на договорной основе юридических лиц, имеющих лицензии на право проведения работ в области защиты информации;

– совместно с Ответственным за обеспечение безопасности ПДн вносить предложения по совершенствованию деятельности *МКОУ «Липковская СОШ № 2»* в области обеспечения безопасности ПДн при их обработке.

Ответственный за организацию обработки ПДн обязан:

– осуществлять внутренний контроль за соблюдением работниками Учреждения законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн;

– доводить до сведения работников Учреждения положения законодательства Российской Федерации о ПДн, локальных актов по вопросам обработки ПДн, требований к защите ПДн;

– организовывать прием и обработку обращений запросов субъектов ПДн или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов;

– добросовестно выполнять функции, возложенные на него;

– не разглашать ПДн, полученные в рамках выполнения обязанностей.

Ответственный за организацию обработки ПДн должен знать:

– законодательные и нормативно-правовые акты, методические и нормативные материалы по вопросам, связанным с обеспечением информационной безопасности и безопасности ПДн;

– процессы обработки ПДн, действующие в *МКОУ «Липковская СОШ № 2»*;

– используемые информационные технологии Обработки ПДн;

– систему организации защиты ПДн;

– основы работы и функционирования;

– категории обрабатываемых ПДн, категории субъектов ПДн, работников, допущенных к обработке ПДн.

4. Обязанности ответственного за организацию обработки ПДн в случае обнаружения нарушений

Ответственный за организацию обработки ПДн для проведения расследования привлекает комиссию Учреждения, назначенную приказом *директора МКОУ «Липковская СОШ № 2»*. Комиссия обязана установить, имела ли место утечка ПДн и обстоятельства, ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по обработке ПДн, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования председатель экспертной комиссии принимает решение о наказании виновных лиц инеобходимых мероприятиях по устранению недостатков.

Все структурные подразделения и работники, работающие с ПДн, обязаны содействовать проведению служебной проверки.

Работа с ПДн может возобновляться только после устранения всех выявленных нарушений и нейтрализации их последствий.

5. Ответственность

Ответственный за организацию обработки ПДн несет ответственность (гражданскую, уголовную, административную, дисциплинарную) за неисполнение либо ненадлежащее исполнение должностных обязанностей.

С Инструкцией ознакомлены:

_____	_____	_____
дата	подпись	ФИО