**Муниципальное автономное дошкольное образовательное учреждение «Детский сад комбинированного вида №25 «Рябинка»**

**П Р И К А З**

**18.02.2021 № 20-од**

|  |
| --- |
| Бердск |

**Об утверждении положения**

**об обеспечении безопасности персональных данных**

Во исполнение требований Федерального закона №152-ФЗ от 27 июля 2006 г. «О персональных данных», приказа ФСТЭК России №21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и прочих нормативных документов по защите информации,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных МАДОУ № 25 (далее – Положение) (Приложение к настоящему приказу).
2. Ответственному за обеспечение безопасности персональных данных в информационных системах обеспечить выполнение требований Положения.
3. Требования Положения довести до работников, непосредственно осуществляющих защиту персональных данных в информационных системах персональных данных.
4. Контроль за исполнением настоящего Приказа оставляю за собой.

|  |  |  |
| --- | --- | --- |
|  | Заведующий | Т.Г.Сушкова |

Приложение

к приказу от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 2021 г. № \_\_\_\_\_\_

**ПОЛОЖЕНИЕ**

**об обеспечении безопасности персональных данных,**

**обрабатываемых в информационных системах персональных данных**

**МАДОУ № 25**

1. **Термины и определения**
	1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.
	2. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
	3. Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
	4. Основные технические средства и системы – технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи персональных данных.
	5. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
	6. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);
	7. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
	8. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
	9. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
2. **Общие положения**
3. Настоящее Положение об обеспечении безопасности персональных данных, обрабатываемых в информационных системах персональных данных
МАДОУ № 25 (далее – Положение), разработано в соответствии с законодательством Российской Федерации о персональных данных (далее – ПДн) и нормативными правовыми актами (методическими документами) федеральных органов исполнительной власти по вопросам безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн).
4. Настоящее Положение определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.
5. Положение обязательно для исполнения всеми работниками
МАДОУ № 25 (далее – Учреждение), непосредственно осуществляющими защиту ПДн, обрабатываемых в ИСПДн.
6. **Цели и задачи обеспечения безопасности персональных данных**
7. Основной целью обеспечения безопасности ПДн, при их обработке в ИСПДн, является защита ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.
8. Задачей, которую необходимо решить для достижения поставленной цели, является обеспечение безопасности ПДн при их обработке в ИСПДн с помощью системы защиты персональных данных (далее – СЗПДн), нейтрализующей актуальные угрозы, определенные в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006г. №152-ФЗ «О персональных данных».
9. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в ИСПДн.
10. **Основные принципы построения системы защиты информации**
11. СЗПДн основывается на следующих принципах:
* системности;
* комплексности;
* непрерывности защиты;
* разумной достаточности;
* гибкости;
* простоты применения средств защиты информации (далее – СЗИ).
1. Принцип системности – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.
2. Принцип комплексности – предполагает, что СЗПДн должна включать совокупность объектов защиты, сил и средств, принимаемых мер, проводимых мероприятий и действий по обеспечению безопасности ПДн от возможных угроз всеми доступными законными средствами, методами и мероприятиями.
3. Принцип непрерывности защиты – это процесс обеспечения безопасности ПДн, осуществляемый руководством, ответственным за обеспечение безопасности ПДн в ИСПДн и работниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность СЗИ, сколько процесс, который должен постоянно идти на всех уровнях внутри Учреждения, и каждый работник должен принимать участие в этом процессе.
4. Принцип разумной достаточности – предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.
5. Принцип гибкости – СЗПДн должна быть способна реагировать на изменения внешней среды и условий осуществления своей деятельности.
6. Принцип простоты применения СЗИ – механизмы защиты должны быть интуитивно понятны и просты в применении. Применение СЗИ не должно быть связано со знанием каких-либо языков или требовать дополнительных затрат на её применение, а также не должно требовать выполнения рутинных малопонятных операций.
7. **Основные мероприятия по обеспечению безопасности персональных данных**
8. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, проводятся следующие мероприятия:
* определение ответственных лиц за обеспечение защиты ПДн;
* определение актуальных угроз безопасности ПДн;
* определение уровня защищенности ПДн;
* реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн;
* ограничение доступа в помещения, где размещены основные технические средства и системы, позволяющие осуществлять обработку ПДн;
* учет и хранение съемных машинных носителей ПДн;
* организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ;
* организация парольной защиты;
* организация антивирусной защиты;
* организация обновления программного обеспечения и СЗИ;
* использование СЗИ;
* использование средств шифровальной (криптографической) защиты информации (далее – СКЗИ);
* оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн;
* обнаружение фактов несанкционированного доступа к ПДн и принятие мер;
* контроль за принимаемыми мерами по обеспечению безопасности ПДн;
* планирование мероприятий по защите ПДн в ИСПДн;
* управление (администрирование) СЗПДн;
* управление конфигурацией ИСПДн и СЗПДн;
* реагирование на инциденты;
* информирование и обучение персонала ИСПДн.
1. Определение ответственных лиц за обеспечение безопасности ПДн
	1. За вопросы обеспечения безопасности ПДн, обрабатываемых в ИСПДн, отвечают:
* Заведующий.
* Ответственный за организацию обработки ПДн – работник, отвечающий за организацию и состояние процесса обработки ПДн.
* Ответственный за обеспечение безопасности ПДн в ИСПДн – работник, отвечающий за правильность использования и нормальное функционирование установленной СЗПДн.
* Администратор ИСПДн – работник, отвечающий за правильность использования и бесперебойное, стабильное функционирование установленных систем обработки ПДн.
1. Определение актуальных угроз безопасности ПДн в ИСПДн
	1. Актуальные угрозы безопасности ПДн, обрабатываемых в ИСПДн, определяются по результатам оценки возможностей (потенциала, оснащенности и мотивации) внешних и внутренних нарушителей, анализа возможных уязвимостей ИСПДн, возможных способов реализации угроз безопасности ПДн и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).
	2. Для определения угроз безопасности ПДн и разработки «Модели угроз безопасности персональных данных» применяются методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом
	4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от
	16 августа 2004 г. №1085.
2. Определение уровня защищенности ПДн
	1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется в соответствии с постановлением Правительства Российской Федерации от
	1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и оформляется в виде «Акта об определения уровня защищенности персональных данных».
3. Реализация правил разграничения доступа и введение ограничений на действия пользователей ИСПДн
	1. Реализация правил разграничения доступа, к ПДн, обрабатываемым в ИСПДн, осуществляется в соответствии с «Положением о разрешительной системе доступа в информационных системах персональных данных
	МАДОУ № 25», утвержденным приказом заведующего Учреждения.
	2. Основные технические средства и системы ИСПДн располагаются в помещениях, находящихся в пределах границы контролируемой зоны, определенной приказом заведующего Учреждения, с максимальным удалением от её границ.
	3. Доступ в помещения, в которых ведется обработка ПДн, осуществляется в соответствии с «Правилами доступа работников в помещения, в которых ведется обработка персональных данных в МАДОУ № 25», утвержденными приказом заведующего Учреждения.
4. Учет и хранение съемных машинных носителей ПДн
	1. Работа со съемными машинными носителями ПДн в ИСПДн осуществляется в соответствии с «Порядком обращения со съемными машинными носителями персональных данных в МАДОУ № 25», утвержденным приказом заведующего Учреждения.
5. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ.
	1. Организация резервирования и восстановления работоспособности программного обеспечения, баз данных ПДн и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией по организации резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных МАДОУ № 25», утвержденной приказом заведующего Учреждения.
6. Организация парольной защиты
	1. Организация парольной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по парольной защите информации в МАДОУ № 25», утвержденной приказом заведующего Учреждения.
7. Организация антивирусной защиты
	1. Организация антивирусной защиты в ИСПДн осуществляется в соответствии с «Инструкцией по организации антивирусной защиты в
	МАДОУ № 25», утвержденной приказом заведующего Учреждения.
8. Организация обновления программного обеспечения и СЗИ
	1. Организация обновления программного обеспечения и СЗИ в ИСПДн осуществляется в соответствии с «Инструкцией ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных МАДОУ № 25» и «Инструкцией администратора информационных систем персональных данных МАДОУ № 25», утвержденные приказом заведующего Учреждения.
9. Применение СЗИ
	1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, применяются СЗИ, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации, в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. №184-ФЗ «О техническом регулировании».
	2. Установка и настройка СЗИ в ИСПДн проводится в соответствии с эксплуатационной документацией на СЗПДн и документацией на СЗИ.
10. Использование СКЗИ
	1. Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, при их передаче по открытым каналам связи, применяются СКЗИ. Обращение с СКЗИ, эксплуатируемыми в ИСПДн, осуществляется в соответствии с «Инструкцией по обращению со средствами криптографической защиты информации в
	МАДОУ № 25», утвержденной приказом заведующего Учреждения.
11. Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию СЗПДн
	1. На этапах внедрения СЗПДн проводится оценка эффективности принимаемых мер по обеспечению безопасности ПДн, которая включает в себя:
* предварительные испытания СЗПДн;
* опытную эксплуатацию СЗПДн;
* анализ уязвимостей ИСПДн и принятие мер по их устранению;
* приемочные испытания СЗПДн.
1. Обнаружение фактов несанкционированного доступа к ПДн и принятие мер
	1. Ответственному за обеспечение безопасности ПДн в ИСПДн или администратору ИСПДн должны сообщаться любые инциденты информационной безопасности, в которые входят:
* факты попыток и успешной реализации несанкционированного доступа в ИСПДн;
* факты попыток и успешной реализации несанкционированного доступа в помещения, в которых ведется обработка ПДн;
* факты сбоя или некорректной работы систем обработки ПДн;
* факты сбоя или некорректной работы СЗИ;
* факты разглашения ПДн, обрабатываемых в ИСПДн;
* факты разглашения информации о методах и способах защиты и обработки ПДн в ИСПДн.
	1. Разбор инцидентов информационной безопасности проводится в соответствии с «Регламентом реагирования на инциденты информационной безопасности в информационных системах персональных данных МАДОУ № 25», утвержденным приказом заведующего Учреждения.
1. Контроль за принимаемыми мерами по обеспечению безопасности ПДн
	1. Контроль за принимаемыми мерами по обеспечению безопасности ПДн осуществляется в соответствии с «Регламентом проведения внутреннего контроля соответствия обработки персональных данных в
	МАДОУ № 25», утвержденным приказом заведующего Учреждения.
2. **Ответственность**
3. Все работники, допущенные в установленном порядке к работе с ПДн, несут административную, материальную, уголовную ответственность в соответствии с действующим законодательством Российской Федерации за необеспечение сохранности и несоблюдение правил работы с ПДн.
4. Ответственность за доведение требований настоящего Положения до работников Учреждения и обеспечение мероприятий по их реализации несет ответственный за обеспечение безопасности ПДн в ИСПДн.

ЛИСТ ОЗНАКОМЛЕНИЯ

с приказом МАДОУ № 25 от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2021 г. № \_\_\_\_\_\_

«Об утверждении положения об обеспечении безопасности персональных данных»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Фамилия имя отчество | Должность | Дата ознакомления | Подпись |
| 1 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 2 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 3 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 4 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 5 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 6 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 7 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 8 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 9 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 10 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 11 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 12 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 13 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 14 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 15 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 16 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 17 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 18 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 19 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |
| 20 |  |  | «\_\_\_» \_\_\_ 20\_\_ г. |  |