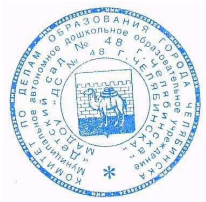
Муниципальное автономное дошкольное образовательное учреждение
«Детский сад № 48 г. Челябинска»



Подписан: МАДОУ "ДС №48 Г. ЧЕЛЯБИНСКА"
DN: ИНН=007448228924, СНИЛС=07856778843, ОГРН=1207400041265, E=olg-yusupova83@mail.ru, T=Заведующий, OU=Общее подразделение, O="МАДОУ ""ДС №48 Г. ЧЕЛЯБИНСКА""", STREET=ул. Маршала Чуйкова 25Б, L=Челябинск, S=74 Челябинская область, C=RU, G=Ольга Александровна, SN=Бура, CN="МАДОУ "" ДС №48 Г. ЧЕЛЯБИНСКА"""
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: место подписания
Дата: 2021-08-03 13:15:37
Foxit PhantomPDF Версия: 9.7.5

УТВЕРЖДАЮ
Заведующий МАДОУ
«ДС № 48 г. Челябинска»
_____ О. А. Бура
Приказ № 03-01/02-ПДн
от 09.03.2021 г.

ИНСТРУКЦИЯ
администратора безопасности информационных систем персональных данных

1.Общие положения

1.1. Настоящая Инструкция определяет общие функции, права и ответственность лица, ответственного за обеспечение безопасности информационных систем персональных данных (далее – Ответственный) в МАДОУ «ДС № 48 г. Челябинска» (далее – ДОУ).
1.2. Настоящая инструкция разработана в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.
1.3. Ответственный назначается приказом руководителя ДОУ на основании «Положения о разграничении прав доступа к обрабатываемым персональным данным в МАДОУ «ДС № 48 г. Челябинска».
1.4. Ответственный подчиняется непосредственно руководителю ДОУ.
1.5. Ответственный отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе ПДн, при их обработке в ИСПДн ДОУ.
1.6. Ответственный осуществляет методическое руководство деятельностью пользователей ИСПДн ДОУ по вопросам обеспечения безопасности информации.
1.7. Требования Ответственного, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДн ДОУ.
1.8. Ответственный несет персональную ответственность за качество проводимых им работ по контролю действий должностных лиц ДОУ при работе в ИСПДн ДОУ, состояние и поддержание установленного уровня защищенности информации, обрабатываемой в ИСПДн ДОУ.
1.9. Ответственный в своей работе руководствуется настоящей Инструкцией, Политикой информационной безопасности ДОУ, другими регламентирующими документами ДОУ, руководящими и нормативными документами регуляторов Российской Федерации в области обеспечения безопасности персональных данных.

2. Задачи
администратора безопасности информационных систем персональных данных

Основными задачами администратора безопасности информации являются:
2.1. Поддержание необходимого уровня защищенности ИСПДн ДОУ от несанкционированного доступа (далее – НСД) к информации.
2.2. Обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации.
2.3. Установка средств защиты информации и контроль выполнения правил их эксплуатации.
2.4. Сопровождение средств защиты информации (далее – СЗИ) от НСД и основных технических средств и систем (далее – ОТСС) ИСПДн ДОУ.

2.5. Периодическое обновление СЗИ и проведение комплекса мероприятий по предотвращению нарушений требований информационной безопасности (далее – ИБ).
2.6. Оперативное реагирование на нарушения требований по ИБ в ИСПДн ДОУ и участие в их предотвращении (нейтрализации).

В рамках выполнения основных задач администратор безопасности информационных систем персональных данных осуществляет:
- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических СЗИ;
- текущий контроль технологического процесса автоматизированной обработки ПДн;
- участие в проведении служебных расследований фактов нарушений или угрозы нарушений безопасности ПДн;
- контроль соблюдения нормативных требований по защите информации, обеспечения комплексного использования технических средств, методов и организационных мероприятий по безопасности информации в структурных подразделениях ДОУ;
- методическую помощь пользователям ИСПДн ДОУ по вопросам обеспечения безопасности ПДн.

3. Обязанности администратора безопасности информационных систем персональных данных

Администратор безопасности информации обязан:
3.1.Знать и выполнять требования нормативных документов по защите информации, регламентирующих порядок защиты информации, обрабатываемой в ИСПДн ДОУ.
3.2. Участвовать в установке, настройке и сопровождении программных средств защиты информации.
3.3. Участвовать в приемке новых программных средств обработки информации.
3.4. Обеспечить доступ к защищаемой информации пользователям ИСПДн ДОУ согласно их правам доступа при получении оформленного соответствующим образом разрешения (заявки).
3.5. Уточнять в установленном порядке обязанности пользователей ИСПДн ДОУ при обработке ПДн.
3.6. Вести контроль осуществления резервного копирования информации.
3.7. Анализировать состояние защиты ИСПДн ДОУ.
3.8. Контролировать правильность функционирования средств защиты информации и неизменность их настроек.
3.9. Контролировать физическую сохранность технических средств обработки информации.
3.10. Контролировать исполнение пользователями ИСПДн ДОУ введенного режима безопасности, а также правильность работы с элементами ИСПДн ДОУ и средствами защиты информации.
3.11. Контролировать исполнение пользователями ИСПДн ДОУ правил парольной политики.
3.12. Периодически анализировать журнал учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей ИСПДн ДОУ и выявления возможных нарушений.
3.13. Не допускать установку, использование, хранение и размножение в ИСПДн ДОУ программных средств, не связанных с выполнением функциональных задач.
3.14. Осуществлять периодические контрольные проверки автоматизированных рабочих мест ИСПДн ДОУ.
3.15. Оказывать помощь пользователям ИСПДн ДОУ в части применения СЗИ и консультировать по вопросам введенного режима защиты.
3.16. Периодически представлять руководству отчет о состоянии СЗИ ИСПДн ДОУ, о нештатных ситуациях и допущенных пользователями нарушениях установленных требований по защите информации.

3.17. В случае отказа работоспособности технических средств и программного обеспечения ИСПДн ДОУ, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.
3.18. В случае выявления нарушений режима безопасности информации (ПДн), а также возникновения внештатных и аварийных ситуаций принимать необходимые меры с целью ликвидации их последствий.
3.19. Принимать участие в проведении работ по оценке соответствия ИСПДн ДОУ требованиям безопасности информации.

4. Права администратора безопасности информационных систем персональных данных

Администратор безопасности информации имеет право:
4.1. Отключать от ресурсов ИСПДн ДОУ пользователей, осуществивших НСД к защищаемым ресурсам ИСПДн ДОУ или нарушивших другие требования по ИБ.
4.2. Давать сотрудникам обязательные для исполнения указания и рекомендации по вопросам ИБ.
4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, несанкционированного доступа, утраты, порчи защищаемой информации и технических средств ИСПДн ДОУ.
4.4. Организовывать и участвовать в любых проверках по использованию пользователями ДОУ телекоммуникационных ресурсов.
4.5. Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн ДОУ при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.
4.6. Осуществлять взаимодействие с руководством и персоналом ДОУ по вопросам обеспечения ИБ.
4.7. Запрещать устанавливать на серверах и автоматизированных рабочих местах нештатное программное и аппаратное обеспечение.
4.8. Запрашивать и получать от пользователей ИСПДн ДОУ информацию и материалы, необходимые для организации своей работы.
4.9. Вносить на рассмотрение руководства предложения по улучшению состояния ИБ ПДн, обрабатываемых в ДОУ.

5. Ответственность администратора безопасности информационных систем персональных данных

Администратор безопасности несет ответственность за:
5.1. Организацию защиты информационных ресурсов и технических средств ИСПДн ДОУ.
5.2. Качество проводимых работ по контролю действий пользователей администраторов ИСПДн, состояние и поддержание необходимого уровня защищенности информационных и технических ресурсов ИСПДн ДОУ.
5.3. Разглашение сведений ограниченного доступа (коммерческая тайна, персональные данные и иная защищаемая информация), ставших известными ему по роду работы.

6. Действия администратора безопасности информационных систем персональных данных при обнаружении попыток НСД

6.1. К попыткам НСД относятся: сеансы работы с телекоммуникационными ресурсами ДОУ незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции доступа к определенным данным или манипулирования ими; действия третьего лица, пытающегося получить доступ (или получившего доступ) к информационным ресурсам ИСПДн ДОУ с использованием учетной записи администратора или другого пользователя ИСПДн, в целях получения

коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.
6.2. При выявлении факта (попытки) НСД администратор безопасности обязан: прекратить доступ к информационным ресурсам со стороны выявленного участка НСД: доложить заведующему ДОУ о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях; известить заведующего ДОУ, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД; проанализировать характер НСД; по решению комиссии ДОУ осуществить действия по выяснению причин, приведших к НСД; предпринять меры по предотвращению подобных инцидентов в дальнейшем.

С инструкцией ознакомлен(а), 2-й экземпляр на руки получил(а):

Администратор безопасности информационных систем персональных данных

_____ _____
(Подпись) (Расшифровка подписи)