

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ДОШКОЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДЕТСКИЙ САД № 38
ПУШКИНСКОГО РАЙОНА САНКТ- ПЕТЕРБУРГА**

ул. Вишерская д.3, кор.1, поселок Шушары, Санкт-Петербург, Россия, 196626,
ОКПО 111111671 ОГРН 1127847464425, ИНН/КПП 7820329797/782001001

ПРИКАЗ

02.09.2022

№ 03-02-01-71

**О назначении ответственных
за защиту информации**

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 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», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17

ПРИКАЗЫВАЮ:

1. Назначить ответственным за организацию обработки персональных данных в ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга документоведа Новикову И.В.
2. На время отсутствия ответственного лица Новиковой И.В. (отпуск, болезнь) обязанности исполняет специалист по охране труда Кравчук А.В.
3. Утвердить инструкцию ответственного за организацию обработки персональных данных в ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга согласно приложению № 1.
4. Назначить ответственным за организацию и обеспечение информационной безопасности (безопасности персональных данных) заместителя заведующего по АХЧ Темежникову И.С.
5. Утвердить инструкцию ответственного за обеспечение безопасности персональных данных в ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга согласно приложению № 2
6. Назначить администратором безопасности информации специалиста по охране труда Кравчук А.В.
7. Утвердить инструкцию администратора безопасности информации ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга согласно приложению № 3.
8. Признать утратившими силу:
 - 8.1. Приказ № 03-02-01/25 от 16.03.2020 «О назначении ответственного за организацию обработки персональных данных».
9. Выше указанным сотрудникам дать письменное согласие на работу, не входящую в должностные обязанности, за дополнительную плату в соответствии с Положением об установлении доплат, надбавок и иных выплат материального стимулирования работников ГБДОУ детский сад №38 пушкинского района СПб.
9. Контроль за исполнением приказа оставляю за собой.

Заведующий

Я.Л.Егорова

Инструкция
ответственного за организацию обработки персональных данных
в ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга

1. Общие положения.

1.1. Должностная инструкция ответственного за организацию обработки персональных данных (далее - Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных", Федеральным законом от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", постановлением Правительства Российской Федерации от 21.03.2012 № 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", другими нормативными правовыми актами.

1.2. Инструкция определяет ответственность, обязанности и права лица, назначенного ответственным за организацию обработки персональных данных.

1.3. Ответственный за организацию обработки персональных данных осуществляет руководство работой ответственного за обеспечение безопасности персональных данных в ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга (далее ГБДОУ).

2. Должностные обязанности

Ответственный за организацию обработки персональных данных обязан:

2.1. Определить порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных.

2.2. Определять порядок и условия применения средств защиты информации.

2.3. Анализировать эффективность применения мер по обеспечению безопасности персональных данных.

2.4. Контролировать состояние учета машинных носителей персональных данных.

2.5. Проверять соблюдение правил доступа к персональным данным.

2.6. Контролировать проведение мероприятий по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.7. Обеспечивать конфиденциальность персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля.

3. Права

Ответственный за организацию обработки персональных данных имеет право:

3.1. Осуществлять проверки по контролю соответствия обработки персональных данных требованиям к защите персональных данных.

3.2. Запрашивать у сотрудников администрации информацию, необходимую для реализации полномочий.

3.3. Требовать от ответственных должностных лиц за обработку персональных данных уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных.

3.4. Применять меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации.

3.5. Вносить заведующему предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

3.6. Вносить заведующему предложения о привлечении к дисциплинарной ответственности работников администрации, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

4. Ответственность

Ответственный за организацию обработки персональных данных несет ответственность:

4.1. За осуществление внутреннего контроля за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, доведение до сведений работников соответствующих структурных подразделений положений законодательства Российской Федерации о персональных данных, правовых актов ГБДОУ по вопросам обработки персональных данных, требований к защите персональных данных, организации приема и обработки обращений и осуществлению контроля за приемом и обработкой таких обращений.

4.2. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим трудовым законодательством Российской Федерации.

5. Порядок пересмотра инструкции

5.1. Настоящая Инструкция пересматривается, изменяется и дополняется по мере необходимости, но не реже одного раза в три года.

5.2. С приказом о внесении изменений (дополнений) в настоящую Инструкцию знакомятся под расписку все сотрудники ГБДОУ, на которых распространяется действие этой инструкции.

Инструкция
ответственного за обеспечение безопасности персональных данных
в ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга

1. Общие положения.

1.1. Данная должностная инструкция лица, ответственного за обеспечение безопасности персональных данных в ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга (далее - Инструкция) определяет общие функции, ответственность, права и обязанности ответственного за обеспечение безопасности персональных данных в ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга (далее – ГБДОУ).

1.2. Ответственный за обеспечение безопасности персональных данных (далее – Ответственный) является сотрудником ГБДОУ и назначается приказом заведующего.

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

1.4. Решение вопросов обеспечения безопасности персональных данных входит в прямые служебные обязанности ответственного за обеспечение безопасности персональных данных.

1.5. Ответственный за обеспечение безопасности персональных данных обладает правами доступа к любым программным и аппаратным ресурсам, а также во все помещения, где ведется обработка персональных данных.

1.6. Ответственный в своей работе руководствуется настоящей Инструкцией, Политикой в отношении обработки персональных данных, другими регламентирующими документами, руководящими и нормативными документами регуляторов Российской Федерации в области обеспечения безопасности персональных данных.

1.7. Руководство работой Ответственного осуществляется ответственным за организацию обработки персональных данных в ГБДОУ.

2. Должностные обязанности

Ответственный за обеспечение безопасности персональных данных обязан:

2.1. Соблюдать требования законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, «Правил обработки персональных данных» и других нормативных документов ГБДОУ в области обработки и защиты персональных данных.

2.2. Поддерживать необходимый уровень защищенности (режим безопасности) персональных данных при их обработке в ИСПДн согласно «Положение о защите персональных данных при их обработке».

2.3. Осуществлять методическое руководство всех групп пользователей в вопросах функционирования СЗИ и введенного режима защиты.

2.4. Уточнять в установленном порядке обязанности всех групп пользователей ИСПДн по обеспечению безопасности персональных данных.

2.5. Контролировать исполнение всем группами пользователей ИСПДн парольной политики.

2.6. Знать перечень персональных данных и технических средств, входящих в информационные системы персональных данных (далее – ИСПДн) ГБДОУ.

2.7. Организовать учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных. Своевременно анализировать журнал учёта событий, регистрируемых СЗИ, с целью выявления возможных нарушений.

2.8. Недопускать установку, использование, хранение и размножение в ИСПДн

программного обеспечения, не связанного с выполнением функциональных задач.

2.9. Представлять на утверждение список лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему.

2.10. Доводить до сведения сотрудников ГБДОУ положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.11. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ ИСПДн.

2.12. Не допускать к работе на элементах ИСПДн посторонних лиц.

2.13. Предлагать заведующему мероприятия по совершенствованию работы по защите персональных данных.

2.14. По указанию заведующего своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах, касающихся обеспечения безопасности ПДн.

2.15. Осуществлять контроль выполнения требований локальных нормативных актов по защите ПДн сотрудниками ГБДОУ.

2.16. Обеспечивать контроль действий администратора безопасности ИСПДн по обеспечению информационной безопасности.

2.17. Проводить разбирательства 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.

2.18. Обеспечить прекращение обработки персональных данных пользователям информационной системы при обнаружении нарушений порядка обработки персональных данных.

2.19. Участвовать в работе комиссии по уничтожению персональных данных.

2.20. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.

2.21. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ.

2.22. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления НСД к информации и техническим средствам АРМ.

3. Права

Ответственный за обеспечение безопасности персональных данных имеет право:

3.1. Требовать от пользователей информационных ресурсов выполнения требований локальных нормативных актов по защите персональных данных, в том числе выполнение инструкций, а также проводить проверку соблюдения данных требований.

3.2. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

3.3. Участвовать в анализе ситуаций, касающихся функционирования СЗИ, и в расследованиях по случаям несанкционированного доступа к персональным данным и другим случаям нарушения режима обработки персональных данных.

4.4. Вносить предложения заведующему по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

5. Ответственность

Ответственный несет ответственность:

5.1. За качество проводимых работ по контролю всех групп пользователей ИСПДн в вопросах обеспечения безопасности персональных данных.

5.2. За обеспечение устойчивой работоспособности СЗИ ИСПДн.

5.3. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, в пределах, определенных действующим трудовым законодательством Российской Федерации.

6. Порядок пересмотра инструкции

6.1. Настоящая Инструкция пересматривается, изменяется и дополняется по мере необходимости, но не реже одного раза в три года.

6.2. С приказом о внесении изменений (дополнений) в настоящую Инструкцию знакомятся под расписку все сотрудники ГБДОУ, на которых распространяется действие этой инструкции.

Инструкция
администратора безопасности информации
ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга

1. Общие положения

1.1. Настоящая Инструкция определяет обязанности должностного лица, администратора безопасности информации (в том числе персональных данных (ПДн), обрабатываемой в информационных системах ПДн (ИСПДн) ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга, (далее - администратор безопасности).

1.2. Действие настоящей Инструкции распространяется в ГБДОУ детский сад №38 Пушкинского района Санкт-Петербурга (далее – ГБДОУ).

1.3. Администратор безопасности назначается приказом заведующего.

1.4. Руководство работой администратора безопасности по вопросам обеспечения безопасности информации осуществляет ответственный за обеспечение безопасности информации в ГБДОУ.

1.5. Администратор безопасности отвечает за поддержание установленного уровня безопасности защищаемой информации, в том числе ПДн, при их обработке в ИСПДн.

1.6. Администратор безопасности осуществляет методическое руководство деятельностью пользователей ИСПДн в вопросах обеспечения безопасности информации.

1.7. Требования администратора безопасности, связанные с выполнением им своих обязанностей, обязательны для исполнения всеми пользователями ИСПДн ГБДОУ.

2. Задачи администратора безопасности

2.1. Основными задачами администратора безопасности являются:

- поддержание необходимого уровня защиты ИСПДн от несанкционированного доступа (НСД) к информации;
- обеспечение конфиденциальности обрабатываемой, хранимой и передаваемой по каналам связи информации;
- установка средств защиты информации и контроль выполнения правил их эксплуатации;
- сопровождение средств защиты информации (СЗИ) от НСД и основных технических средств и систем (ОТСС) ИСПДн;
- периодическое обновление СЗИ и комплекса мероприятий по предотвращению инцидентов ИБ;
- оперативное реагирование на нарушения требований по ИБ в ИСПДн и участие в их прекращении.

2.2. В рамках выполнения основных задач администратор безопасности 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;
- методическую помощь всем работникам по вопросам обеспечения безопасности ПДн.

3. Обязанности администратора безопасности информации

Администратор безопасности обязан:

3.1. 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.

3.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения (ПО) автоматизированных рабочих мест (АРМ) и серверов (операционные системы, прикладное и специальное);

- аппаратных средств;

- аппаратных и программных средств защиты.

3.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

3.4. Осуществлять контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

3.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

3.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.7. Проводить периодический контроль принятых мер по защите, в пределах возложенных на него функций.

3.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля пользователем ИСПДн.

3.9. Обеспечивать постоянный контроль за выполнением пользователями установленного комплекса мероприятий безопасности информации.

3.10. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

3.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

3.12. Обеспечивать строгое выполнение требований безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

3.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн, сторонними физическими людьми и организациями.

3.14. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

3.15. Не допускать к работе на рабочих станциях и серверах посторонних лиц.

3.16. Осуществлять контроль монтажа оборудования сторонних организаций.

3.17. Участвовать в приемке для нужд ГБДОУ новых программных средств.

3.18. Обобщать результаты своей деятельности и готовить предложения по ее совершенствованию.

3.19. При изменении конфигурации автоматизированной системы вносить соответствующие изменения в паспорт АС, обрабатывающей информацию ограниченного доступа.

4. Права администратора безопасности

Администратор безопасности имеет право:

4.1. Отключать от ресурсов ИСПДн администрации работников, осуществивших НСД к защищаемым ресурсам ИСПДн или нарушивших другие требования по ИБ.

4.2. Давать работникам обязательные для исполнения указания и рекомендации по вопросам ИБ.

4.3. Инициировать проведение служебных расследований по фактам нарушений установленных требований обеспечения ИБ, НСД, утраты, порчи защищаемой информации и технических средств ИСПДн.

4.4. Организовывать и участвовать в любых проверках по использованию пользователями телекоммуникационных ресурсов.

4.5. Осуществлять контроль информационных потоков, генерируемых пользователями ИСПДн при работе с корпоративной электронной почтой, съемными носителями информации, подсистемой удаленного доступа.

4.6. Осуществлять взаимодействие с заведующим и сотрудниками 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 сотрудников связанных с ПДн информацию и материалы, необходимые для организации своей работы.

4.9. Вносить на рассмотрение заведующего предложения по улучшению состояния ИБ ПДн, обрабатываемых в ГБДОУ.

5. Ответственность администратора безопасности

Администратор безопасности несет ответственность:

5.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими локальными организационно-распорядительными документами, в соответствии с действующим трудовым законодательством Российской Федерации.

5.2. За качество проводимых работ по контролю действий пользователей и администраторов ИСПДн, состояние и поддержание необходимого уровня защиты информационных и технических ресурсов ИСПДн.

5.3. За разглашение сведений ограниченного доступа (коммерческая тайна, персональные данные и иная защищаемая информация), ставших известными ему по роду работы.

6. Действия администратора безопасности при обнаружении попыток НСД

6.1. К попыткам НСД относятся:

- сеансы работы с телекоммуникационными ресурсами 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 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 ГБДОУ ИБ о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

- проанализировать характер НСД;

- по решению заведующего ГБДОУ ИБ осуществить действия по выяснению причин, приведших к НСД;

- предпринять меры по предотвращению подобных инцидентов в дальнейшем.

7. Порядок пересмотра инструкции

7.1. Настоящая Инструкция пересматривается, изменяется и дополняется по мере необходимости, но не реже одного раза в три года.

7.2. С приказом о внесении изменений (дополнений) в настоящую Инструкцию знакомятся под расписку все сотрудники ГБДОУ, на которых распространяется действие этой инструкции.

С приказом №03-02-01-71 «О назначении ответственных за защиту информации» от 02.09.2022 ознакомлены:

Ф.И.О.	Дата	Подпись
Кравчук А.В.		
Темежникова И.С.		
Новикова И.В.		