

Принята

Общим собранием работников ОО
протокол от 04.09.2019 №4

Утверждена

приказом от 14.10.2019 №163-ОД
Директор
_____ Л. Н. Демьянчук

**ПОЛОЖЕНИЕ
О ПОДРАЗДЕЛЕНИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ**

1. Общие положения

1.1. Настоящее Положение о подразделении по защите информации (далее – Положение) в государственном бюджетном общеобразовательном учреждении школе № 755 «Региональный Центр аутизма» Василеостровского района Санкт-Петербурга (далее - ОО) является официальным документом, в котором в соответствии с Концепцией информационной безопасности информационной системы персональных данных ОО, Политикой информационной безопасности информационной системы персональных данных ОО, положением об обработке и защите персональных данных в ОО определяются условия обеспечения безопасности персональных данных в ОО:

1.1.1. Разработано в соответствии с:

- Конституцией Российской Федерации;
- Федеральным законом от 30.11.1994 №51-ФЗ «Гражданский кодекс Российской Федерации» (с изменениями);
- Федеральным законом от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации» (с изменениями);
- Федеральным законом от 01.04.1996 №27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» (с изменениями);
- Федеральным законом от 31.05.1996 № 61-ФЗ «Об обороне» (с изменениями);
- Федеральный закон от 26.02.1997 № 31-ФЗ «О мобилизационной подготовке и мобилизации в Российской Федерации» (с изменениями);
- Федеральным законом от 28.03.1998 №53 «О воинской обязанности и военной службе» (с изменениями);
- Федеральный закон от 31.07.1998 №146-ФЗ «Налоговый кодекс Российской Федерации» (с изменениями);
- Федеральным законом от 15.12.2001 №167-ФЗ «Об обязательном пенсионном страховании в РФ» (с изменениями);
- Федеральный закон от 30.12.2001 № 197-ФЗ «Трудовой кодекс Российской Федерации», ст. 85-90;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями);
- Федеральным Законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» (с изменениями);
- Федеральным законом от 29.12.2006 № 255-ФЗ «Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством» (с изменениями);
- Федеральным законом от 28.12.2013 №400-ФЗ «О страховых пенсиях» (с изменениями);
- Федеральным законом от 29.12.2012 № 273-ФЗ (ред. от 29.12.2017) "Об образовании в Российской Федерации" (с изменениями);
- Законом Санкт-Петербурга от 22.11.2011 №728-132 «Социальный кодекс Санкт-Петербурга» (с изменениями);
- Законом Санкт-Петербурга от 17.07.2013 №461-ФЗ «Об образовании в Санкт-Петербурге» (с изменениями);
- Постановлением Правительства РФ от 16.04.2003 №225 (с изменениями) «О трудовых книжках»;
- Постановлением Госкомстата РФ от 05.01.2004 №1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты»;
- Постановлением Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Постановлением Правительства Санкт-Петербурга от 17.02.2009 № 149 "О мерах по реализации Закона Санкт-Петербурга "Об общем образовании";
- Постановлением Правительства РФ от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановление Правительства РФ от 06.07.2008 № 512 (с изменениями) "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных";

- Распоряжением Комитета по транспорту Санкт-Петербурга от 27.06.2007 № 31-р "О видах проездных билетов и порядке их обращения" (с изменениями);
- Распоряжением Комитета по образованию от 25.10.2013 №2453-р "О работе с автоматизированными информационными системами, базами данных и иными электронными информационными ресурсами образовательных организаций Санкт-Петербурга" (с изменениями);
- Распоряжением Комитета по образованию от 04.02.2014 №313-р "О работе с автоматизированными информационными системами, базами данных и иными электронными информационными ресурсами дошкольных образовательных организаций Санкт-Петербурга" (с изменениями)
- Распоряжением Комитета по образованию Санкт-Петербурга от 10.09.2010 №1616-р "О внедрении комплексной автоматизированной информационной системы каталогизации ресурсов образования";
- Приказом Минобрнауки России от 22.01.2014 № 32 "Об утверждении Порядка приема граждан на обучение по образовательным программам начального общего, основного общего и среднего общего образования" (с изменениями);
- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с изменениями);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г. (ДСП);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.2008 г. (ДСП);
- Уставом ОО.
 - 1.1.2. Определяет:
 - основные цели, функции, права подразделения по защите информации;
 - обеспечение комплексной защиты информации, содержащей персональные данные;
 - установление ответственности должностных лиц, отвечающих за защиту информации, за невыполнением требований норм, регулирующих защиту персональных данных.
 - 1.1.3. Принимаются общим собранием работников ОО и утверждается приказом директора ОО.
 - 1.1.4. Является локальным нормативным актом, регламентирующим деятельность ОО.
 - 1.1.5. Принимается на неопределенный срок.

2. Цель и задача подразделения по защите информации

1. **Основная цель** деятельности подразделения по защите информации - обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных ОО.
- 2.2. **Задачи** подразделения по защите информации:
 - принятие правовых, организационных и технических мер, направленных на осуществление режима защиты персональных данных;
 - взаимодействие с сотрудниками ОО по вопросам защиты персональных данных в пределах своей компетенции;
 - оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных.

3. Состав подразделения по защите информации

- 3.1. Подразделение по защите информации комплектуется специалистами, имеющими инженерно-техническое образование.
- 3.2. Руководство подразделением защиты информации осуществляет руководитель подразделения, назначаемый приказом директора ОО.

4. Основные направления деятельности подразделения по защите информации

К основным направлениям деятельности подразделения относятся:

- 4.1. Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.
- 4.2. Определение и постановка задач по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты персональных данных (далее – ПДн) в ОО.
- 4.3. Планирование, организация и выполнение работ по защите информации в ОО.
- 4.4. Проведение проверок информационных систем персональных данных, рабочих мест на право проведения работ по обработке персональных данных.
- 4.5. Проведение периодического контроля эффективности мер защиты информации в ОО. Учет и анализ результатов контроля.
- 4.6. Разработка нормативно-методических и распорядительных документов по защите информации в ОО.
- 4.7. Соблюдение конфиденциальности информации ограниченного доступа и реализация права на доступ к информации.

5. Основные функции подразделения по защите информации

5.1. Аттестация объектов, помещений, технических средств, программ, алгоритмов на предмет соответствия требованиям защиты ПДн по соответствующим классам безопасности.

5.2. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.3. Соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией. Настройка и эксплуатация системы защиты в соответствии с организационно-распорядительными документами.

5.4. Недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование.

5.5. Поддержание в актуальном состоянии действующих журналов и форм учета по работе с ПДн. Составление и предоставление в установленном порядке отчетности.

5.6. Проведение специальных исследований и контрольных проверок по выявлению демаскирующих признаков, возможных каналов утечки ПДн, в том числе по техническим каналам.

5.7. Рациональное использование и сохранность компьютерного и иного оборудования, учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных.

5.8. Своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до ответственного за организацию обработки персональных данных в ОО и руководителя ОО.

5.9. Составление актов и другой технической документации о степени защищенности технических средств и помещений.

5.10. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных ОО.

5.11. Определение состава и содержание мер по обеспечению безопасности персональных данных;

5.12. Осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами защиты персональных данных в ОО.

5.13. Взаимодействие с операторами персональных данных по вопросам защиты информации, в том числе:

5.13.1. Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

5.13.2. Участие в расследовании нарушений в области защиты информации в ОО и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений.

5.13.3. Разбирательство и составление заключений по фактам несоблюдения условий хранения материальных 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, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

6. Документация подразделения

6.1. Акты и другая техническая документация о степени защищенности технических средств и помещений.

6.2. Модель угроз безопасности персональных данных.

6.3. Отчет о результатах проведения внутренней проверки информационной системы персональных данных.

6.4. Перечень применяемых средств защиты информации, эксплуатационной и технической документации к ним.

6.5. План внутренних проверок состояния защиты персональных данных.

6.6. План мероприятий по обеспечению защиты персональных данных.

6.7. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации, связанных с информационной системой персональных данных.

7. Права и ответственность

Должностные лица подразделения:

7.1. Имеют право:

7.1.1. Получать поступающие в учреждение документы и иные информационные материалы по своему профилю деятельности для ознакомления, систематизированного учета и использования в работе.

7.1.2. Запрашивать и получать от руководителя учреждения и структурных подразделений информацию, необходимую для выполнения возложенных на подразделение задач и функций.

7.1.3. Проверять соблюдение законодательства и нормативно-правовых актов по вопросам защиты ПДн в деятельности учреждения.

7.1.4. Вносить предложения руководителю учреждения по совершенствованию форм и методов работы подразделения.

7.1.5. Участвовать в совещаниях при рассмотрении вопросов, связанных с безопасностью обрабатываемых ПДн и иной информации учреждения.

7.2. Несут ответственность за:

7.2.1. Выполнение возложенных на подразделение функций.

7.2.2. Организацию работы подразделения, своевременное и квалифицированное выполнение приказов, распоряжений, поручений директора ОО, действующих нормативно-правовых актов по своему профилю деятельности, качественное ведение документации, предусмотренной действующими нормативно-правовыми документами;

7.2.3. Рациональное и эффективное использование материальных, финансовых и кадровых ресурсов подразделения.

7.2.4. Выполнение своих функциональных обязанностей, состояние трудовой и исполнительской дисциплины подразделения, правил внутреннего распорядка, противопожарной безопасности и техники безопасности.

7.2.5. Предоставление в установленном порядке достоверной статистической и иной информации о деятельности подразделения.

7.2.6. Недопущение использования информации, содержащей персональные данные в неслужебных целях.

8. Заключительные положения

8.1. Положение о подразделении по защите информации вступает в силу с момента его утверждения и действует бессрочно.

8.2. Изменения и дополнения к настоящему Положению принимаются общим собранием работников ОО и утверждаются приказом директора ОО.

8.3. После принятия новой редакции Положения о подразделении по защите информации предыдущая редакция утрачивает силу.

ГБОУ № 755 САНКТ-ПЕТЕРБУРГА "РЕГИОНАЛЬНЫЙ ЦЕНТР АУТИЗМА", Демьянчук Лариса Николаевна, Директор
12.04.2021 19:26 (MSK), Сертификат № 011CA8BD00E2AB0EA64A6C50F6ECD12D79