ПРИНЯТО
Общим собранием работников
ГБДОУ детский сад №6
протокол №1 от 03.09.2018 года
Председатель собрания
_____Е.Е.Кияниченко

СОГЛАСОВАНО
С профсоюзным комитетом
ГБДОУ детский сад №6
протокол №1 от 03.09.2018 года
Председатель профсоюзного комитета
_____А.О.Кузьмина

УТВЕРЖДЕНО
приказом Заведующего ГБДОУ
детского сада №6
№56/1-Д от 03.09.2018 года
_____Е.Е.Кияниченко

Положение
о порядке обработки и обеспечении безопасности персональных данных
в Государственном бюджетном дошкольном образовательном
учреждении детском саду № 6 общеразвивающего вида
Кронштадтского района Санкт-Петербурга

Санкт-Петербург
2018 г.

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и устанавливает единый порядок обработки персональных данных в ГБДОУ детском саду № 6 Кронштадтского района Санкт-Петербурга (далее – ГБДОУ № 6).

1.2. В целях настоящего Положения используются следующие термины и понятия:

- персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- 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;
- информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее – персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2. Основные условия проведения обработки персональных данных

2.1. Обработка персональных данных осуществляется:

- после получения согласия субъекта персональных данных, составленного по форме согласно Приложению №1 (относится к персоналу ГБДОУ № 6),
- после получения согласия субъекта персональных данных, составленного по форме согласно Приложению №2 (относится к родителю/законному представителю воспитанника ГБДОУ № 6), и к настоящему Положению, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона;
- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по городу Санкт-Петербургу, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона;
- после принятия необходимых мер по защите персональных данных в соответствии с Положением о защите персональных данных воспитанников (Приложение №3) и Положением о защите персональных данных работников (Приложение №4)

2.2. В органе исполнительной власти и подведомственных им учреждениях приказом руководителя назначается сотрудник, ответственный за организацию обработки персональных данных, с которым заключается дополнительное соглашение (Приложение №5), свою работу ответственный за обработку персональных данных в ДОУ осуществляет в соответствии с должностной инструкцией (Приложение №6). Также определяется перечень лиц, допущенных к обработке персональных данных (Приложение №7).

2.3. Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящим Положением, Положением о разграничении прав доступа к персональным данным (Приложение №8) и подписывают обязательство о неразглашении информации, содержащей персональные данные, по форме согласно Приложению №9 к настоящему Положению.

2.4. В случае прекращения трудовых обязательств с лицами, допущенными к обработке персональных данных, оформляется обязательство работника о не разглашении персональных

данных, ставших известными ему в связи с исполнением должностных обязанностей (Приложение №10).

2.5. Запрещается обрабатывать персональные данные в присутствии лиц, не допущенных к их обработке.

2.6. В случае отказа от обработки персональных данных при приеме на работу заполняется отзыв согласия на обработку персональных данных (Приложение №11) и дается разъяснение субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в связи с поступлением на работу (Приложение № 12).

2.7. В случае отзыва субъектом персональных данных согласия на их обработку, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных (Приложение №13).

2.8. В случае изменения персональных данных субъекта, предоставляются документы, являющиеся основанием внесения изменения и составляется дополнительное соглашение в двух экземплярах – Приложение №14.

3. Порядок определения защищаемой информации

3.1. В органе исполнительной власти на основании «Перечня сведений конфиденциального характера», утвержденного Указом Президента Российской Федерации от 06.03.1997 № 188, определяется и утверждается перечень сведений ограниченного доступа, не относящихся к государственной тайне (далее - конфиденциальной информации) – Приложение №15 и перечень информационных систем персональных данных – Приложение №16.

3.2. На стадии проектирования каждой ИСПД определяются цели и содержание обработки персональных данных, утверждается перечень обрабатываемых персональных данных.

4. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

4.1. Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

4.2. Оператором осуществляется определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПД) в соответствии с требованиями постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в зависимости от типа и объема обрабатываемых персональных данных, а также типа угроз (модель угроз – Приложение №17).

4.3. Мероприятия безопасности персональных данных на стадиях проектирования и ввода в эксплуатацию объектов информатизации проводятся в соответствии с требованиями постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» – Приложение №18.

4.4. Не допускается обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации при отсутствии:

- утвержденных организационно-технических документов о порядке эксплуатации информационных систем персональных данных, включающих акт классификации ИСПД (Приложение №19), инструкции пользователя (Приложение №20), администратора по организации антивирусной защиты (Договор с ООО «Мастеркомп №1/18 от 15.12.2017года), и других нормативных и методических документов;
- настроенных средств защиты от несанкционированного доступа, средств антивирусной

защиты, резервного копирования информации и других программных и технических средств в соответствии с требованиями безопасности информации;
- охраны и организации режима допуска в помещения, предназначенные для обработки персональных данных.

5. Порядок обработки персональных данных без использования средств автоматизации

5.1. Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка персональных данных) в соответствии с постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы банных) на электронных носителях информации.

5.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

5.3. При неавтоматизированной обработке персональных данных на бумажных носителях:
- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо не совместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

5.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовые формы), должны соблюдаться следующие условия:
- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, – при необходимости получения письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;
- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

5.5. Неавтоматизированная обработка персональных данных в электронном виде осуществляется на внешних носителях информации.

5.6. При отсутствии технологической возможности осуществления неавтоматизированной обработки персональных данных в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к персональным данным лиц, не допущенных к их обработке.

5.7. При несовместимости целей неавтоматизированной обработки персональных данных, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;
- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

5.8. Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

5.9. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

6. Ответственность должностных лиц

При обнаружении нарушений в работе сотрудников ГБДОУ № 6 в сфере защиты персональных данных составляется Акт выявленных нарушений – Приложение №21, сведения о нарушении заносятся в Журнал выявленных нарушений – Приложение №22.

Работники, допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 1
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

СОГЛАСИЕ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Субъект персональных данных (далее - Получатель):
Фамилия, имя, отчество:_____
Адрес:_____
Паспорт серия/№:_____
Выдан орган/дата:_____
_____
_____
Код подразделения: _____
2. Оператор:
   2.1. Государственное бюджетное дошкольное образовательное учреждение детский сад № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга.
   Адрес: 197760, г. Санкт-Петербург, гор. Кронштадт, Цитадельское шоссе, д.2а; 197760, г. Санкт-Петербург, гор. Кронштадт, ул. Флотская, д.10а.
   2.2. Санкт-Петербургское государственное казенное учреждение «Централизованная бухгалтерия администрации Кронштадтского района Санкт-Петербурга».
   Адрес: 197760, г. Санкт-Петербург, гор. Кронштадт, ул. Мартынова, д.2/59, литер А.

Цели обработки Персональных данных: ведение базы данных, издание приказов и совершение иных действий, порождающих юридические последствия в связи с возникновением трудовых отношений.

3. Получатель в целях соблюдения законодательства Российской Федерации настоящим дает согласие своей волей и в своем интересе на обработку перечисленных ниже Персональных данных:
   3.1. Фамилия, имя, отчество (в том числе имевшиеся ранее), дата рождения (год, месяц, дата), место рождения (республика, край, область, район, город), гражданство, адрес места жительства или место пребывания (республика, край, область, район, город, улица, дом, корпус, квартира), сведения о документе, удостоверяющем личность, сведения о дате выдачи указанного документа и выдавшем его органе, номер страхового свидетельства государственного пенсионного страхования, семейное, социальное, имущественное положение, образование, специальность, квалификация, сведения о доходах, о составе семьи, о трудовой деятельности, номера телефонов (домашнего, мобильного), сведения о постановке на налоговый учет (ИНН), и др.
   3.2. Любые иные данные и информация, которые могут потребоваться Оператору в связи с осуществлением целей, указанных в п.3 (Далее - Персональные данные).

4. Получатель настоящим дает согласие Оператору на совершение с Персональными данными перечисленных ниже действий:
   4.1. Обработку Персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.
   4.2. Общее описание используемых Оператором способов обработки персональных данных:
   4.2.2. При обработке Персональных данных Оператор принимает необходимые организационные и технические меры для защиты Персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения Персональных данных, а также от иных неправомерных действий.

4.2.3. Получатель уведомлен о том, что он (она) в любой момент времени, письменно обратившись к Оператору, вправе запросить перечень имен и адресов любых получателей Персональных данных, ознакомиться с Персональными данными, обратиться с просьбой о предоставлении дополнительной информации в отношении хранения и обработки Персональных данных или же потребовать внесения любых необходимых изменений в Персональные данные для их уточнения.

4.3. Ряд персональных данных публикуется на сайте ГБДОУ детского сада № 6, а именно:

- фамилия, имя, отчество – для помощника воспитателя;
- фамилия, имя, отчество, фотография, стаж работы, образование, курсы повышения квалификации – для заведующего, заместителя заведующего, воспитателя.

Указанные персональные данные становятся общедоступными.

5. Срок, порядок отзыва:

Настоящее согласие действует на период действия заключенного трудового договора №_____ от «____»_____года или до момента отзыва его мной по письменному заявлению.

В подтверждение вышеизложенного, нижеподписавшийся Получатель подтверждает свое согласие на обработку своих Персональных данных в соответствии с тем, как это описано выше.

Дата «_____»_____20___ г.

_____(ФИО, печатными буквами)

Подпись Получателя:_____

Приложение № 2
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6
УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

СОГЛАСИЕ РОДИТЕЛЯ (ЗАКОННОГО ПРЕДСТАВИТЕЛЯ) НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ СВОИХ И НЕСОВЕРШЕННОЛЕТНЕГО

Я,_____
(фамилия, имя и отчество (при наличии) полностью)
зарегистрированн____ по адресу_____

паспорт серия_____№_____, выдан (кем и когда) _____

в соответствии с п. 1 ст. 9 закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных» даю Государственному бюджетному дошкольному образовательному учреждению детскому саду № 6 Кронштадтского района Санкт-Петербурга (далее - ГБДОУ д/с №6), находящемуся по адресу: 197760, г. Санкт-Петербург, гор. Кронштадт, улица Флотская, дом 10а свое согласие на обработку моих персональных данных, а именно:

- фамилия, имя, отчество;
- данные паспорта;
- адрес регистрации и адрес проживания;
- данные о составе семьи;
- данные дополнительных документов, при необходимости их предоставления в ДОУ, таких, например, как свидетельства о рождении старших детей не достигших 18-летнего возраста, свидетельство о заключении брака, данные документа о смене фамилии, справки об инвалидности члена семьи, сведения о доходах семьи и др., которые могут понадобиться для предоставления компенсации части родительской платы или невзимания родительской платы за присмотр и уход за ребенком. В этом случае они указываются в соответствующем заявлении.

и в соответствии со ст. 64 п. 1 «Семейного кодекса РФ» – для родителей; для усыновителей – ст. 64 п. 1, ст. 137 п. 1 «Семейного Кодекса РФ», опекуны – ст. 15 п. 2 Федерального закона «Об опеке и попечительстве», попечители - ст. 15 п. 3. Федерального закона «Об опеке и попечительстве», даю согласие на обработку персональных данных несовершеннолетнего ребенка_____,
(фамилия, имя, отчество (при наличии) несовершеннолетнего ребенка полностью)
родивше____ся «_____» _____ 20_____года зарегистрированного по адресу:
_____

на основании свидетельства о рождении/постановления об установлении опеки/ др. – нужное подчеркнуть серия _____№_____, выданного (кем и когда)_____

Давая это согласие, я действую добровольно и в интересах несовершеннолетнего.

Лица, осуществляющие обработку персональных данных в ГБДОУ д/с №6: заведующий Кияниченко Елена Евгеньевна; делопроизводитель Федорова Елена Владимировна; педагогический состав группы, в которую зачислен ребёнок.

Согласие дается мной в отношении обработки следующих персональных данных несовершеннолетнего:

- фамилия, имя, отчество;
- дата и место рождения;
- пол;
- адрес регистрации и адрес проживания;
- сведения о гражданстве;

- сведения о составе семьи;
- данные свидетельства о рождении несовершеннолетнего;
- данные страхового свидетельства обязательного пенсионного страхования;
- сведения о состоянии здоровья несовершеннолетнего;
- данные страхового медицинского полиса несовершеннолетнего;
- данные медицинской карты (формы 026/у-2000).

Я даю согласие на использование персональных данных моего ребенка исключительно в следующих целях:

- соблюдения порядка и правил приема детей в образовательные учреждения;
- обеспечения организации учебного процесса для ребенка;
- формирования индивидуальных сведений о воспитанниках;
- обеспечения безопасности воспитанников;
- статистической обработки данных.

Допускаются следующие действия в отношении персональных данных несовершеннолетнего:

– сбор, систематизация, накопление, хранение, уточнение (обновление, изменение) данных;
– использование при обработке только в указанных выше целях, обезличивание, блокирование (не включает возможность ограничения моего доступа к персональным данным ребенка), уничтожение;
– передача третьим лицам при обмене информацией в рамках действующего законодательства в сфере образования;
– опубликование персональных данных на интернет-ресурсах ГБДОУ д/с № 6, а именно: фотографий мероприятий в обезличенной форме в качестве отчетной информации о результатах деятельности; опубликование внутренних приказов также исключительно в обезличенной форме.

Обработку допускается осуществлять как неавтоматизированным, так и автоматизированным способами.

Неавтоматизированным способом (на бумажной основе или при обработке данных вручную) обработка производится в «Журнале приёма заявлений о приёме в ГБДОУ д/с №6», в «Книге учёта движения воспитанников», при формирования личных дел воспитанников, обработка с использованием программ Microsoft Office Word и Microsoft Office Excel.

Автоматизированным способом допускается обработка:

– в автоматизированной информационной системе «Параграф:ДОУ» предназначенной для автоматизации процессов управления образовательным учреждением, а так же автоматизации процессов учета и сбора данных на дошкольном уровне управления системой образования;
– в автоматизированной информационной системе «Электронный детский сад» для учета детей зарегистрированных в очереди для зачисления в дошкольное образовательное учреждение.

Совместно с ГБДОУ д/с №6 операторами персональных данных воспитанников ГБДОУ д/с №6 являются:

– Санкт-Петербургское государственное казенное учреждение «Централизованная бухгалтерия администрации Кронштадтского района Санкт-Петербурга» (далее - ГКУ ЦБ); лицо, осуществляющее обработку персональных данных – бухгалтер ГКУ ЦБ по ГБДОУ д/с № 6 – Кирьянова Наталья Николаевна; адрес местоположения: 197760, г. Санкт-Петербург, гор. Кронштадт, ул. Мартынова, д.2/59, литер А; телефон: 8 (812) 576-83-20. Персональные данные воспитанников передаются в ГКУ ЦБ от ГБДОУ д/с №6 при зачислении ребенка в ДОУ.
– Санкт-Петербургское государственное бюджетное учреждение здравоохранения «Городская поликлиника №74», «Детское поликлиническое отделение №55» (далее – ДПО №55), лица, осуществляющие обработку персональных данных – врач: Егорова Лидия Ивановна, медицинская сестра: Коротина Лидия Владимировна; приём ведется в медицинском кабинете ГБДОУ д/с №6. Персональные данные воспитанников передаются сотрудникам ДПО №55 от ГБДОУ д/с №6 при зачислении ребенка в ДОУ.

Данное Согласие действует до завершения обучения несовершеннолетнего или до момента отзыва его мной по письменному заявлению.

Дата: «_____»_____20_____ года.

Подпись:_____/_____

(подпись) *(фамилия и инициалы)*

Приложение № 3
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Положение об обработке и защите персональных данных воспитанников Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга

1. Общие положения

1.1. Настоящее Положение устанавливает порядок получения, учета, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным воспитанников Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга (далее – ГБДОУ детский сад № 6) и их родителей (законных представителей).

1.2. Цель настоящего Положения – защита персональных данных воспитанников ГБДОУ детский сад № 6 и их родителей (законных представителей) от несанкционированного доступа, а также обеспечение их неприкосновенности и сохранности. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

1.3. Основанием для разработки настоящего Положения являются Конституция РФ, Трудовой кодекс РФ, Федеральный закон от 27 июля 2006 №152-ФЗ «О персональных данных**».**

1.4. Настоящее Положение и изменения к нему утверждаются заведующим ГБДОУ детского сада № 6 и вводятся его приказом. Все работники ГБДОУ детского сада № 6 должны быть ознакомлены под роспись с данным Положением и изменениями к нему.

1.5. Положение действует до принятия нового.

2. Состав персональных данных

2.1. Персональные данные воспитанника, его родителей (законных представителей) - сведения о фактах, событиях и обстоятельствах жизни воспитанника, его родителей (законных представителей), позволяющие идентифицировать его личность, необходимые администрации дошкольного учреждения в связи с осуществлением образовательной деятельности.

2.2. При определении объема и содержания персональных данных воспитанника администрация руководствуется Конституцией Российской Федерации, федеральными законами и настоящим Положением.

2.3. Администрация ГБДОУ детского сада № 6 может получить от родителей (законных представителей) воспитанников следующие данные:

- фамилия, имя, отчество, дата рождения, место жительства воспитанника;
- фамилия, имя, отчество, самих родителей (законных представителей) воспитанника;
- данные направления, выданного комиссией по комплектованию дошкольных учреждений;
- контактные телефоны;
- сведения о месте работы (учебы) родителей (законных представителей);
- данные свидетельства обязательного пенсионного страхования;
- данные медицинской карты ребенка (форма 026/у);
- данные полиса обязательного медицинского страхования;
- данные сертификата о прививках (при наличии);
- сведения о месте регистрации и о месте проживания ребенка;
- иные персональные данные воспитанника, необходимые в связи с отношениями обучения и воспитания.

К таким данным относятся документы, содержащие сведения, необходимые для

предоставления воспитаннику гарантий и компенсаций, установленных действующим законодательством:

- документы о составе семьи;
- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.).

2.4. В согласии на обработку персональных данных отдельным пунктом дается согласие или несогласие на включение персональных данных воспитанника в общедоступные источники персональных данных.

2.5. Персональные данные воспитанника и его родителей являются конфиденциальной информацией и не могут быть использованы администрацией или любым иным лицом в личных целях или передаваться третьим лицам.

3. Получение, хранение, обработка и передача персональных данных воспитанника

3.1. Порядок получения персональных данных:

3.1.1. Родитель (законный представитель) предоставляет руководителю или работнику, имеющему допуск к персональным данным воспитанника, достоверные сведения о себе и своём ребёнке, а так же оригиналы и копии требуемых документов.

3.1.2. Все персональные данные воспитанников, их родителей (законных представителей) дошкольного учреждения следует получать у самого родителя (законного представителя).

3.1.3. Способы получения персональных данных воспитанников:

- ксерокопирование оригиналов документов;
- внесение сведений в учетные формы на бумажных и (или) электронных носителях;
- получение оригиналов необходимых документов.

Способы получения персональных данных родителей (законных представителей):

- заключение договора с указанием необходимых для этого персональных данных;
- ксерокопирование оригиналов документов;

3.1.4. В случаях, когда администрация может получить необходимые персональные данные воспитанника только у третьего лица, администрация должна уведомить об этом одного из родителей (законного представителя) заранее и получить от него письменное согласие.

3.1.5. Родитель (законный представитель) подписывает Согласие (Приложение №1) на обработку своих персональных данных и данных своего ребенка.

3.1.6. Администрация дошкольного учреждения обязана сообщить одному из родителей (законному представителю) о целях и способах обработки и защиты персональных данных, а также о возможных последствиях отказа одного из родителей (законного представителя) дать письменное согласие на их обработку.

3.1.7. Согласие родителя (законного представителя) на обработку своих персональных данных и своего ребёнка может быть отозвано путем направления родителем (законным представителем) письменного заявления не менее чем за 3 дня до момента отзыва согласия.

3.1.8. Работник дошкольного учреждения не имеет права получать и обрабатывать персональные данные воспитанника и родителя (законного представителя) о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, интимной жизни.

3.1.9. Согласие родителя (законного представителя) не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия руководителя;
- персональные данные являются общедоступными по требованию полномочных государственных органов в случаях, предусмотренных федеральным законодательством;

- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных.

3.2. Принципы обработки персональных данных:

- законности целей и способов обработки персональных данных и добросовестности;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям оператора;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
- достоверности персональных данных, их достаточности для целей обработки.

3.3. Порядок обработки, передачи и хранения персональных данных:

3.3.1. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, определенного законодательством – все персональные данные, хранящиеся в электронном виде уничтожаются сразу после завершения обучения в ДОУ; личное дело передается в архив, где по истечении 3 лет хранения уничтожается.

3.4. При передаче персональных данных воспитанника и родителя (законного представителя) Заведующий или работники, имеющие допуск к персональным данным, должны соблюдать следующие требования:

3.4.1. Не сообщать персональные данные воспитанника или родителя (законного представителя) третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью воспитанника или родителя (законного представителя), а также в случаях, установленных федеральными законами.

3.4.2. Предупредить лиц, получивших персональные данные воспитанника или родителя (законного представителя), о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные воспитанника или родителя (законного представителя), обязаны соблюдать режим секретности (конфиденциальности).

3.4.3. Разрешать доступ к персональным данным воспитанника или родителя (законного представителя) только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные воспитанника или родителя (законного представителя), которые необходимы для выполнения конкретной функции.

3.4.4. При размещении распорядительного акта при зачислении воспитанника в образовательную организацию на официальном сайте организации исключать персональные данные, кроме фамилии и инициалов.

3.5. Определить, что право доступа к персональным данным воспитанников и родителей (законных представителей) в ГБДОУ детском саду № 6 имеют: заведующий, заместитель заведующего, воспитатели, документовед, ответственный за безопасность персональных данных.

3.6. К обработке персональных данных воспитанников и их родителей допускаются:

- заведующий;
- заместитель заведующего;
- медицинские работники;
- воспитатели;
- делопроизводитель;
- бухгалтер.

Каждый из вышеперечисленных сотрудников даёт расписку о неразглашении персональных данных.

3.7. Хранение и использование документированной информации персональных данных воспитанника или родителя (законного представителя):

3.7.1. Персональные данные воспитанника или родителя (законного представителя) могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде.

3.7.2. Персональные данные воспитанников и родителей (законных представителей) хранятся в местах с ограниченным доступом к этим документам:

– место хранения личных дел воспитанников ГБДОУ детского сада № 6 – кабинет заведующего;

– медицинские карты воспитанников хранятся в медицинском кабинете, ключи от кабинетов находятся у медицинских работников;

– сведения о воспитанниках и их родителях, необходимые воспитателям для обучения и обеспечения личной безопасности воспитанников, хранятся в рабочем столе воспитателя.

3.7.3. Персональные данные воспитанников и их родителей (законных представителей) хранятся также в информационных системах на персональных компьютерах заведующего и делопроизводителя. Персональные компьютеры защищены от несанкционированного доступа паролем. Защита целостности персональных данных обеспечивается наличием лицензионного программного обеспечения, в том числе антивирусного.

4. Права и обязанности родителей (законных представителей) воспитанников ГБДОУ детского сада № 6 Кронштадтского района Санкт-Петербурга

4.1. В целях обеспечения защиты персональных данных, хранящихся в дошкольном учреждении, родители (законные представители) имеют право на бесплатное получение полной информации о:

- лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

-перечне обрабатываемых персональных данных и источниках их получения;

-сроках обработки персональных данных, в т.ч. срока их хранения.

4.2. Родители (законные представители) имеют право на:

- бесплатное получение полной информации о своих персональных данных и обработке этих данных;

- свободный бесплатный доступ к своим персональным данным, в т.ч. на получение копии любой записи, содержащей персональные данные своего ребёнка, за исключением случаев, предусмотренных федеральным законом;

- требование об исключении или исправлении неверных персональных данных;

- требование об извещении руководителем всех лиц, которым ранее были сообщены неверные или неполные персональные данные воспитанника или родителя (законного представителя), обо всех произведённых в них исключениях, исправлениях или дополнениях.

4.3. Родители (законные представители) не должны отказываться от своих прав на сохранение и защиту тайны.

4.4. В целях обеспечения достоверности своих персональных данных и своих детей родители (законные представители) обязаны:

- при оформлении в дошкольное учреждение представлять о себе и своём ребёнке достоверные сведения в порядке и объёме, предусмотренном настоящим Положением и законодательством РФ;

- в случае изменения своих персональных данных и своего ребёнка, указанных в п. 2.2 настоящего Положения сообщать об этом делопроизводителю в разумные сроки.

5. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

5.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных воспитанника и родителя (законного представителя), привлекаются к дисциплинарной и материальной ответственности, а также привлекаются к гражданско-правовой, административной ответственности в порядке, установленном федеральными законами.

Приложение № 4
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Положение об обработке и защите персональных данных работников Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга

1. Общие положения

1.1. Целью данного Положения является защита персональных данных работников от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано на основании статей Конституции РФ, Трудового Кодекса РФ, Кодекса об административных правонарушениях РФ, Гражданского Кодекса РФ, Уголовного Кодекса РФ, а также Федерального закона «Об информации, информатизации и защите информации».

1.3. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 50 лет срока хранения, если иное не определено законом.

1.4. Настоящее Положение утверждается и вводится в действие приказом заведующего ГБДОУ № 6 и является обязательным для исполнения всеми работниками, имеющими доступ к персональным данным сотрудников.

2. Понятие и состав персональных данных

2.1. Персональные данные работника - информация, необходимая работодателю в связи с трудовыми отношениями и касающиеся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность.

2.2. В состав персональных данных работника и документов, содержащих персональные данные, входят:

- анкетные и биографические данные;
- образование;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность,
- занимаемая должность;
- наличие судимостей
- адрес места жительства;
- домашний телефон;
- место работы или учебы членов семьи и родственников;
- содержание трудового договора;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;

- копии отчетов, направляемые в органы статистики;
- страховое свидетельство государственного пенсионного страхования;
- свидетельство о присвоении ИНН;
- сведения о контактных телефонах.

2.3. Данные документы и сведения являются конфиденциальными, хотя, учитывая их массовость и единое место обработки и хранения - соответствующий гриф ограничения на них не ставится.

3. Обработка персональных данных

3.1. Под обработкой персональных данных работника понимается получение, хранение, комбинирование, передача или любое другое использование персональных данных работника.

3.2. В целях обеспечения прав и свобод человека и гражданина работодатель и его представители при обработке персональных данных работника обязаны соблюдать следующие общие требования:

3.2.1. Работник подписывает Согласие на обработку своих персональных данных (Приложение №1).

3.2.2. Обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

3.2.3. При определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым Кодексом и иными федеральными законами.

3.2.4. Получение персональных данных может осуществляться как путем представления их самим работником, так и путем получения их из иных источников.

3.2.5. Персональные данные следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а так же о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.2.6. Работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни работника (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны работодателем только с его письменного согласия.

3.2.7. Работодатель не имеет право получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.3. К обработке, передаче и хранению персональных данных работника могут иметь доступ следующие работники:
- заведующий ГБДОУ детского сада № 6;
- заместитель заведующего ГБДОУ детского сада № 6;
- сотрудники бухгалтерии;
- делопроизводитель;
- сотрудник, ответственный за безопасность персональных данных;
- старший воспитатель.

3.4. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.4.1. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

3.5. Передача персональных данных работника возможна только с согласия работника или в случаях, прямо предусмотренных законодательством.

3.5.1. При передаче персональных данных работника работодатель должен соблюдать следующие требования:

- не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;
- не сообщать персональные данные работника в коммерческих целях без его письменного согласия;
- предупредить лиц, получающих персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами;
- разрешать доступ к персональным данным работников только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- передавать персональные данные работника представителям работников в порядке, установленном Трудовым Кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

3.5.2. Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

3.5.3. При передаче персональных данных работника потребителям (в том числе и в коммерческих целях) за пределы организации работодатель не должен сообщать эти данные третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника или в случаях, установленных федеральным законом.

3.6. Все меры конфиденциальности при сборе, обработке и хранении персональных данных сотрудника распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

3.7. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

3.8. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

3.9. При принятии решений, затрагивающих интересы работника, работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения. Работодатель учитывает личные качества работника, его добросовестный и эффективный труд.

3.10. Работодатель публикует определенный перечень персональных данных и фотографию работника на сайте учебного заведения в разделе «Сведения об образовательной организации. Руководство и педагогический состав», на что работник дает письменное согласие в соответствующем разделе согласия на обработку персональных данных. А именно:

- фамилия, имя, отчество публикуются для помощников воспитателя;
- для заведующего, заместителя заведующего и воспитателей – фотография, фамилия, имя, отчество, образование, стаж работы, курсы повышения квалификации.

Указанные данные становятся общедоступными.

4. Доступ к персональным данным

4.1. Внутренний доступ (доступ внутри организации).

4.1.1. Право доступа к персональным данным сотрудника имеют:
- заведующий ГБДОУ детского сада № 6;
- заместитель заведующего ГБДОУ детского сада № 6;
- делопроизводитель;
- ответственный за безопасность персональных данных;
- сам работник, носитель данных.
- другие сотрудники организации при выполнении ими своих служебных обязанностей.

4.1.2. Перечень лиц, имеющих доступ к персональным данным работников, определяется приказом заведующего ГБДОУ детского сада № 6.

4.2. Внешний доступ.

4.2.1. К числу массовых потребителей персональных данных вне организации можно отнести государственные и негосударственные функциональные структуры:
- бухгалтерию;
- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления;

4.2.2. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

4.2.3. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

4.2.4. Другие организации.

Сведения о работающем сотруднике или уже уволенном могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

Персональные данные сотрудника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого сотрудника.

В случае развода бывшая супруга/бывший супруг имеют право обратиться в организацию с письменным запросом о размере заработной платы сотрудника без его согласия. (УК РФ).

4.3. Общедоступные персональные данные указаны в разделе 3. пункт 3.10.

5. Защита персональных данных

5.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

5.2. Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

5.3. Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности компании.

5.4. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном федеральным законом.

5.5. "Внутренняя защита".

5.5.1. Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между руководителями и специалистами организации.

5.5.2. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
- воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только заведующему, заместителю заведующего, старшему воспитателю, например, при подготовке материалов для аттестации работника.

5.5.3. Защита персональных данных сотрудника на электронных носителях.

Вычислительная техника, на которой производится обработка, хранение, комбинирование персональных данных должна быть защищена лицензионной антивирусной программой. Все папки, содержащие персональные данные сотрудника, должны быть защищены паролем, который сообщается заведующему ГБДОУ детского сада № 6. Передача персональных данных внутри организации должна осуществляться только с использованием определенных электронных носителей, на которые ведется учет и журнал выдачи.

5.6. "Внешняя защита".

5.6.1. Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

5.6.2. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности компании, посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе, занимающемся персональными данными работников.

5.6.3. Для обеспечения внешней защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- учет и порядок выдачи удостоверений;
- технические средства охраны, сигнализации;
- порядок охраны территории, зданий, помещений, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

5.7. Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

5.8. По возможности персональные данные обезличиваются.

5.9. Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.

6. Права и обязанности работника

6.1. Закрепление прав работника, регламентирующих защиту его персональных данных, обеспечивает сохранность полной и точной информации о нем.

6.2. Работники и их представители должны быть ознакомлены под расписку с документами организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

6.3. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

- требовать исключения или исправления неверных или неполных персональных данных.
- на свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные;
- персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;
- определять своих представителей для защиты своих персональных данных;
- на сохранение и защиту своей личной и семейной тайны.

6.4. Работник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом РФ.
- своевременно сообщать работодателю об изменении своих персональных данных

6.5. Работники ставят работодателя в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

6.6. В целях защиты частной жизни, личной и семейной тайны работники не должны отказываться от своего права на обработку персональных данных только с их согласия, поскольку это может повлечь причинение морального, материального вреда.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.3. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.4. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

7.5. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.5.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера работодатель вправе применять предусмотренные Трудовым Кодексом дисциплинарные взыскания.

7.5.2. Должностные лица, в обязанность которых входит ведение персональных данных сотрудника, обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.5.3. В соответствии с Гражданским Кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.5.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается штрафом, либо лишением права занимать определенные должности или заниматься определенной деятельностью, либо арестом в соответствии с УК РФ.

7.6. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

Приложение № 5
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ № ___

к трудовому договору №_____от «____»_____ _____ года

Государственное бюджетное дошкольное образовательное учреждение детский сад № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга (далее – ГБДОУ № 6), именуемое в дальнейшем «Работодатель», в лице заведующего Кияниченко Елены Евгеньевны, действующего на основании Устава, с одной стороны, и _____, именуем___ в дальнейшем «Работник», с другой стороны, заключили настоящее соглашение о нижеследующем:

1. Дополнить часть __ трудового договора №_____от «_____»_____ _____года пунктом _____следующего содержания:

«Работник назначается ответственным за организацию обработки и защиту персональных данных работников, воспитанников и родителей (законных представителей) воспитанников ГБДОУ № 6: - осуществляет сбор, обработку, накопление, уточнение, систематизацию, обезличивание, уничтожение, хранение персональных данных; - осуществляет внутренний контроль за соблюдением требований законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных; - доводит до сведения работников организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных; - организовывает прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляет контроль за приемом и обработкой таких обращений и запросов».

Настоящее дополнительное соглашение составлено в двух экземплярах, по одному для каждой из сторон, и вступает в силу с «_____»_____20___года.

Оба экземпляра соглашения имеют равную юридическую силу.

Реквизиты сторон:

Работодатель:
Государственное бюджетное дошкольное образовательное учреждение детский сад №6 общеобразовательного вида Кронштадтского района Санкт-Петербурга
ИНН: 7818011037
Юр. адрес:197760, Санкт-Петербург, г. Кронштадт, ул.Флотская , д.10 а
тел 311-37-62

Заведующий ГБДОУ
детского сада № 6_____Е.Е.Кияниченко

М.П.

Работник:
ФИО: _____
_____
Паспортные данные: серия_____№_____
Кем, когда выдан_____
_____
_____
Адрес регистрации:_____
_____

_____/_____/
Подпись расшифровка

«___» _____ 20 ___ г.

Один экземпляр Дополнительного соглашения получил:_____
(дата)

_____ /_____
(подпись) (расшифровка)

Приложение № 6
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Должностная инструкция ответственного лица по организации обработки и защиты персональных данных работников, воспитанников и родителей (законных представителей) воспитанников ГБДОУ детского сада №6 Кронштадтского района Санкт-Петербурга

1. Общие положения

1.1. Настоящая Инструкция разработана для Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга (далее — ГБДОУ детский сад № 6) в соответствии с Конституцией РФ, Трудовым кодексом РФ, Гражданским кодексом РФ, Федеральным законом «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных», ред. от 21.07.2014г., Постановлением Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлении Правительства РФ от17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»; Положением об обработке и защите персональных данных работников, воспитанников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6 (далее — Положение).

1.2. Цель разработки Инструкции — обеспечение защиты прав и свобод работников, воспитанников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6 при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным граждан, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Инструкции.

1.3.1. Настоящая Инструкция вступает в силу с момента ее утверждения заведующим ГБДОУ детского сада № 6 и действует бессрочно, до замены ее новой Инструкцией.

1.3.2. Все изменения в Инструкцию вносятся приказом.

1.4. Ответственные лица должны быть ознакомлены с настоящей Инструкцией под роспись.

1.5. Персональную ответственность за соблюдение всеми ответственными лицами настоящей инструкции, а также контроль за ее соблюдением возложен на заведующего ГБДОУ детского сада № 6.

2. Основные понятия и состав персональных данных.

2.1. Для целей настоящей Инструкции используются следующие основные понятия:

– **персональные данные** — любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, воспитаннику или родителю (законному представителю) воспитанника ДОУ;

– **обработка персональных данных** — сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование и уничтожение персональных данных;

– **конфиденциальность персональных данных** — требование не допускать распространения персональных данных без согласия работников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6 или иного законного основания; данное требование является обязательным для соблюдения назначенного ответственного лица,

получившего доступ к персональным данным работников, воспитанников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6;

– **распространение персональных данных** — действия, направленные на передачу персональных данных работников, воспитанников детского сада № 6 и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6 определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных работников, воспитанников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6; в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным работников, воспитанников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6 каким-либо иным способом;

– **использование персональных данных** — действия (операции) с персональными данными, совершаемые должностным лицом ГБДОУ детского сада № 6 в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении граждан либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

– **блокирование персональных данных** — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

– **уничтожение персональных данных** — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных граждан или в результате которых уничтожаются материальные носители персональных данных граждан;

– **обезличивание персональных данных** — действия, в результате которых невозможно определить принадлежность персональных данных конкретному гражданину;

– **общедоступные персональные данные** — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия гражданина или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

– **информация** — сведения (сообщения, данные) независимо от формы их представления.

– **документированная информация** — зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

– **ИСПД** — Информационные системы персональных данных

2.2. Состав персональных данных.

– фамилия, имя, отчество;
– дата и место рождения;
– паспортные данные;
– сведения об ИНН, СНИЛС;
– адрес проживания (регистрации);
– домашний, контактный телефон;
– семейное, социальное, имущественное положение;
– образование;
– профессия, специальность, занимаемая должность;
– автобиография;
– сведения о трудовом и общем стаже;
– сведения о предыдущем месте работы;
– сведения о воинском учете;
– сведения о социальных льготах;
– размер заработной платы;
– наличие судимостей, ответственности по исполнительному листу;
– содержание трудового договора;
– результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
– привычки и увлечения, в том числе вредные (алкоголь, наркотики и др.);
– реквизиты счёта банковской карты;
– семейное положение;

– прочие сведения, которые могут идентифицировать человека.

2.3. У администрации ГБДОУ детского сада № 6 создаются и хранятся следующие группы документов, содержащие данные о работниках, воспитанниках и родителях (законных представителях) воспитанников ГБДОУ детского сада № 6 в единичном или сводном виде:

– Документы, содержащие персональные данные работников: комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела работников, трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; дела, содержащие материалы служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Учреждения, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения.

– Документация по организации работы с педагогическим и техническим персоналом: положения, должностные инструкции работников, приказы, распоряжения, указания руководства Учреждения; документы по планированию, учету, анализу и отчетности в части работы с персоналом ГБДОУ детского сада № 6.

– Документы, содержащие персональные данные воспитанников: личные дела; медицинские карты-формы 026/у.

– Документы, содержащие персональные данные родителей (законных представителей) воспитанников: данные паспорта; адрес регистрации, (фактического проживания); данные о семейном положении; контактные и рабочие телефоны; сведения о месте работы, занимаемой должности; сведения об образовании; сведения о социальных льготах; сведения о составе семьи; сведения о доходе семьи; сведения о реквизитах банковской карты.

3. Права работников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6.

3.1. Работники и родители (законные представители) воспитанников ГБДОУ детского сада № 6 имеют право:

3.1.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные.

3.1.2. Требовать от ГБДОУ детского сада № 6 уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для ГБДОУ детского сада № 6 персональных данных.

3.1.3. Получать от ГБДОУ детского сада № 6:

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;

– перечень обрабатываемых персональных данных и источник их получения;

– сроки обработки персональных данных, в том числе сроки их хранения;

– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

3.1.4. Требовать извещения ГБДОУ детского сада № 6 всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

3.1.5. Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия ГБДОУ детского сада № 6 при обработке и защите его персональных данных.

3.2. Копировать и делать выписки персональных данных граждан разрешается исключительно в служебных целях с письменного разрешения заведующей.

4. Порядок обработки персональных данных.

4.1. При обработке персональных данных граждан, т.е. их получении, хранении, комбинировании, передаче или любом другом использовании, сотрудники, назначенные

ответственными за обработку персональных данных граждан обязаны соблюдать следующие общие требования:

4.1.1. Обрабатывать персональные данные граждан исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия гражданам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;

4.1.2. Не допускается запрашивать информацию о состоянии здоровья гражданина, за исключением тех сведений, которые относятся к вопросу о возможности выполнения трудовой функции, посещения ГБДОУ детского сада № 6;

4.1.3. Ответственному лицу разрешается доступ только к тем персональным данным сотрудников, которые необходимы для выполнения им его должностных обязанностей;

4.1.4. Ответственное лицо не имеет права получать и обрабатывать персональные данные гражданина о его политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, непосредственно связанных с вопросами трудовых отношений с письменного согласия гражданина, а также случаев предусмотренных федеральным законом.

4.2. Порядок получения персональных данных:

4.2.1. Персональные данные работника и родителя (законного представителя) воспитанника ГБДОУ детского сада № 6 следует получать у него самого, с его письменного согласия.

4.2.2. Согласие работников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6 не требуется в следующих случаях:

– персональные данные являются общедоступными;

– обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

– обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

– обработка персональных данных осуществляется в целях исполнения трудового договора;

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работников, воспитанников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6, если получение его согласия невозможно.

4.2.3 Если персональные данные работника и родителя (законного представителя) воспитанника ГБДОУ детского сада № 6 возможно получить только у третьей стороны, то работник и родитель (законный представитель) воспитанника ГБДОУ детского сада № 6 должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Ответственный должен сообщить работнику и родителю (законному представителю) воспитанника ГБДОУ детского сада № 6 о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.2.4 Все персональные данные воспитанников следует получать от родителей (законных представителей) воспитанников.

4.2.5 Работники, родители (законные представители) воспитанников ГБДОУ детского сада № 6 предоставляют ответственному за обработку и защиту персональных данных достоверные сведения о себе и воспитаннике. Ответственный за обработку и защиту персональных данных проверяет достоверность сведений, сверяя данные, предоставленные работниками и родителями (законными представителями) воспитанников ГБДОУ детского сада № 6, с имеющимися у работников и родителей (законных представителей) воспитанников ГБДОУ детского сада № 6 документами.

5. Хранение персональных данных.

5.1. Персональные данные граждан могут передаваться на хранение на бумажных носителях и в электронном виде — локальной компьютерной сети и компьютерной

программе.

5.2. Персональные данные граждан хранятся у администрации ГБДОУ детского сада № 6; медицинские документы (карты-формы 026/у) хранятся у медицинской сестры.

5.3. Хранение документов, содержащих персональные данные, осуществляется в несгораемых шкафах (сейфах), ключи от которых находятся у заведующей ГБДОУ детского сада № 6, а в его отсутствие у лица его замещающего.

6. Передача персональных данных.

При передаче персональных данных необходимо соблюдать следующие требования:

6.1. Не сообщать персональные данные третьей стороне без письменного согласия гражданина, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью гражданина, а также в случаях, установленных федеральным законом;

6.2. Не сообщать персональные данные в коммерческих целях без письменного согласия гражданина. Обработка персональных данных граждан в целях продвижения работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

6.3. При передаче персональных данных граждан предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лицо, получившее персональные данные гражданина, обязано соблюдать режим секретности (конфиденциальности).

6.4. Ответственный за сбор и обработку персональных данных, должен осуществлять передачу персональных данных граждан в пределах ГБДОУ детского сада № 6 в соответствии с Положением.

7. Защита персональных данных.

7.1. Обеспечение безопасности персональных данных в соответствии с российским законодательством не требуется:

– Для обезличенных персональных данных. Персональные данные могут быть обезличенными, в случае, если над ними были произведены действия, в результате которых невозможно определить их принадлежность конкретному работнику, воспитаннику и/или родителю (законному представителю) воспитанника ГБДОУ детского сада № 6.

– Для общедоступных персональных данных. Персональные данные могут быть общедоступными только с письменного согласия работника и родителя (законного представителя) воспитанника ГБДОУ детского сада № 6. Они могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные работником и/или родителем (законным представителем) воспитанника ГБДОУ детского сада № 6.

7.2. Обязанность по обеспечению безопасности персональных данных при их обработке полностью возлагается на ответственного за обработку и защиту персональных данных.

7.3. Право доступа к персональным данным имеют только ответственные лица, назначенные приказом заведующей:

- заведующий ГБДОУ детского сада № 6;
- заместитель заведующего;
- медицинская сестра;
- воспитатели;
- ответственный за безопасность персональных данных;
- документовед;
- ответственный за функционирование сайта;
- физкультурный руководитель.

7.4. Обработка персональных данных должна проводиться в следующих предназначенных для этого помещениях ГБДОУ детского сада № 6:

- кабинет заведующего;
- кабинет заместителя заведующего;
- кабинет документоведа;
- методический кабинет;

– медицинский кабинет.

7.5. При обработке персональных данных в помещении не должны находиться посторонние лица.

7.6. Ответственные лица должны соблюдать конфиденциальность при обработке персональных данных.

7.7. Ответственные работники должны быть предупреждены о мерах ответственности за разглашение сведений о персональных данных под роспись.

7.8. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

7.9. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

7.10. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

7.11. Обеспечение безопасности персональных данных при их обработке в ИСПД достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование и распространение персональных данных.

7.12. Ответственный обязан:

– проводить мероприятия, направленные на предотвращение несанкционированного доступа (далее НСД) к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

– соблюдать требования парольной защиты (длина пароля должна быть не менее 6 символов; пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения; при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях; ответственный не имеет права сообщать пароль постороннему лицу; полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу, другие обстоятельства) ответственных за обработку и защиту персональных данных и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ПК ГБДОУ детского сада № 6); хранение паролей на бумажном носителе допускается только в сейфе у руководителя учреждения);

– своевременно обнаруживать факты НСД к персональным данным;

– обеспечивать оптимальный уровень антивирусной защиты ИСПД;

– незамедлительно восстанавливать персональные данные, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;

– осуществлять постоянный контроль за обеспечением уровня защищенности персональных данных;

– обеспечивать резервное копирование персональных данных на отчуждаемые носители информации.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных.

8.1. Ответственные ГБДОУ детского сада № 6, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных граждан, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с Федеральными законами РФ и локальными нормативными актами ГБДОУ детского сада № 6.

Приложение № 7
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Перечень лиц, допущенных к обработке персональных данных Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга

№п/п	Должность	Ф.И.О.
1	Заведующий ГБДОУ № 6	Кияниченко Елена Евгеньевна
2	Заместитель Заведующего	Хилюк Алла Владимировна
3	Врач (ДПО №55)	Егорова Лидия Ивановна
4	Медицинская сестра (ДПО №55)	Коротина Лидия Владимировна
5	Старший воспитатель	Комиссарова Юлия Арифовна
6	Делопроизводитель	Федорова Елена Владимировна
7	Инструктор по физической культуре	Кияниченко Нина Алексеевна
8	Музыкальный руководитель	Кириенко Анастасия Дмитриевна
9	Воспитатель	Александрова Екатерина Эдуардовна
10	Воспитатель	Бердник Юлия Сергеевна
11	Воспитатель	Габдельгазизова Ирина Владиковна
12	Воспитатель	Короткая Лина Александровна
13	Воспитатель	Кузьмина Анастасия Олеговна
14	Воспитатель	Лаухина Анна Борисовна
15	Воспитатель	Литвиновская Татьяна Дмитриевна
16	Воспитатель	Монюк Алёна Анатольевна
17	Воспитатель	Павличенко Марина Алексеевна
18	Воспитатель	Подгорная Анна Александровна
19	Воспитатель	Пшеничка Екатерина Сергеевна
20	Воспитатель	Сныткина Светлана Юрьевна
21	Воспитатель	Федорчук Екатерина Александровна
22	Воспитатель	Фролова Юлия Васильевна
23	Воспитатель	Черкасова Елена Ивановна
24	Воспитатель	Якименко Людмила Андреевна

Приложение № 8
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Положение о разграничении прав доступа к обрабатываемым персональным данным в ГБДОУ детском саду № 6 Кронштадтского района Санкт-Петербурга

1. Общие положения

Настоящее Положение о разграничении прав доступа к обрабатываемым персональным данным (далее - Положение) в Государственном бюджетном дошкольном образовательном учреждение детском саду № 6 Кронштадтского района Санкт-Петербурга разработано в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Правилами внутреннего трудового распорядка ГБДОУ № 6 и определяет уровень доступа должностных лиц к персональным данным работников и воспитанников.

2. Основные понятия

Для целей настоящего Положения используются следующие основные понятия:

- ***персональные данные работника*** - любая информация, относящаяся к определенному или определяемому на основании такой информации работнику, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая работодателю в связи с трудовыми отношениями;

- ***персональные данные воспитанников*** - информация, необходимая образовательному учреждению в связи с отношениями, возникающими между обучающимся, его родителями (законными представителями) и образовательным учреждением.

- ***обработка персональных данных*** - сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных;

- ***конфиденциальность персональных данных*** - обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия работника (родителей/законных представителей) воспитанника или иного законного основания;

- ***распространение персональных данных*** - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

- ***использование персональных данных*** - действия (операции) с персональными данными, совершаемые должностным лицом Учреждения в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении работников (обучающихся) либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

- ***блокирование персональных данных*** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи;

- ***уничтожение персональных данных*** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных;

- ***обезличивание персональных данных*** - действия, в результате которых невозможно определить принадлежность персональных данных конкретному работнику (воспитаннику);

- ***информация*** **-** сведения (сообщения, данные) независимо от формы их представления.

3. Разграничение прав доступа при автоматизированной обработке персональных данных

3.1. Разграничение прав осуществляется на основании Отчета по результатам проведения внутренней проверки, а так же исходя из характера и режима обработки персональных данных в информационной системе персональных данных (далее – ИСПДн).

3.2. Список групп должностных лиц ответственных за обработку персональных данных в информационных системах персональных данных, а так же их уровень прав доступа в ИСПДн представлен в таблице № 1

Таблица № 1:

Группа	Уровень доступа к персональным данным	Разрешенные действия
Администратор ИСПДн	- Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. - Обладает полной информацией о технических средствах и конфигурации ИСПДн. - Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. - Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение - распространение - блокирование - обезличивание
Администратор безопасности	- Обладает правами Администратора ИСПДн. - Обладает полной информацией об ИСПДн. - Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. - Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение - распространение - блокирование - обезличивание
Оператор ИСПДн	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем персональным данным.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение - распространение - блокирование - обезличивание

4. Разграничение прав доступа при неавтоматизированной обработке персональных данных

4.1. Разграничение прав осуществляется исходя из характера и режима обработки персональных данных на материальных носителях.

4.2. Список лиц ответственных за неавтоматизированную обработку персональных, а так же их уровень прав доступа к персональным данным представлен в таблице № 2.

Таблица № 2:

Группа	Уровень доступа к персональным данным	Разрешенные действия
Администрация ГБДОУ детского сада № 6: Заведующий Заместитель заведующего	- Обладает полной информацией о персональных данных воспитанников и их родителей, работников ГБДОУ №6. - Имеет доступ к личным делам воспитанников и работников; - Имеет доступ к информации на материальных носителях, содержащей персональные данные воспитанников, их родителей (законных представителей) и работников ГБДОУ №6.	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование - уничтожение - распространение - блокирование - обезличивание
Врач Медицинская сестра (ДПО №55)	- Имеет доступ к личным делам воспитанников, к информации о состоянии здоровья; информации на материальных носителях, содержащей персональные данные воспитанников, их родителей; к личным делам и информации о состоянии здоровья работников ГБДОУ №6.	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование
Старший воспитатель Делопроизводитель	- Имеет доступ к личным делам воспитанников, к информации о состоянии здоровья; информации на материальных носителях, содержащей персональные данные воспитанников, их родителей, работников ГБДОУ №6.	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование
Инструктор по физической культуре Музыкальный руководитель	- Имеет доступ к личным делам воспитанников, к информации о состоянии здоровья; информации на материальных носителях, содержащей персональные данные воспитанников, их родителей.	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование
Воспитатели	- Имеют доступ к личным делам воспитанников своей группы, обладают информацией о персональных данных родителей; - информации на материальных носителях, содержащей персональные данные воспитанников и родителей только **своей группы**.	- сбор и систематизация - накопление и хранение - уточнение (обновление, изменение) - использование - уничтожение

Распространение (передача) информации, содержащей персональные данные, может быть осуществлена только с разрешения администрации ГБДОУ детского сада № 6 в соответствии с Положением о порядке обработки и защиты персональных данных работников и воспитанников ГБДОУ № 6 и в установленном действующим законодательством порядке.

Приложение № 9
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Обязательство о конфиденциальности и неразглашении персональных данных, ставших известными работнику, осуществляющему обработку персональных данных

Я,_____, паспорт серии_____, номер_____, выдан_____
_____
_____
понимаю, что получаю доступ к персональным данным работников и/или воспитанников и родителей воспитанников Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга. В соответствии с Федеральным законом «О персональных данных» от 27 июля 2006 года № 152-ФЗ в период трудовых отношений с организацией и в течение трёх лет после их окончания обязуюсь: не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это требуется в целях предупреждения угрозы жизни и здоровью работника, а так же в случаях установленных федеральным законом; не разглашать сведения, содержащие персональные данные, которые стали известны мне во время исполнения должностных обязанностей; выполнять относящиеся ко мне требования приказов, инструкций и положений по обеспечению безопасности персональных данных; в случае попытки посторонних лиц получить от меня сведения, содержащие персональные данные, обрабатываемые в учреждении, немедленно сообщить директору; в случае моего увольнения все носители персональных данных (рукописи, черновики, диски, дискеты, распечатки, флэш-накопители), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей, передать заведующему; об утрате или недостаче носителей персональных данных, ключей от защищённых помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению персональных данных, а также о причинах и условиях возможной утечки сведений, немедленно сообщить заведующему. Я, предупрежден(а), что, в случае невыполнения любого из вышеуказанных пунктов настоящего обязательства, могу быть привлечен(а) к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

_____/ _____ «____»_____20___г.
(подпись) ФИО дата

Приложение № 10
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Обязательство о конфиденциальности и неразглашении персональных данных, ставших известными работнику, осуществляющему обработку персональных данных, в случае расторжения с ним трудовых отношений.

Я, _____
(фамилия, имя, отчество полностью)
являясь работником _____
(указать наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта (трудового договора).

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных" я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

_____ «____»_____20___г.
(фамилия, инициалы) (подпись) *(дата)*

Приложение № 11
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Заведующему ГБДОУ детского сада № 6
Кронштадтского района Санкт-Петербурга
Елене Евгеньевне Кияниченко
От _____
_____
(фамилия, имя, отчество)
Адрес:_____
_____
_____
Паспорт серии_____№_____
Выдан_____
_____
_____
«_____»_____ _____г
(дата выдачи)

ЗАЯВЛЕНИЕ
(ОТЗЫВ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ)

Я, _____,
(фамилия, имя, отчество полностью)
проживающий по адресу_____,
паспорт серии_____№_____, выдан_____
_____
_____,
(кем, когда выдан)
настоящим, во исполнение требований Федерального закона «О персональных данных», на основании ст. 9 п. 1 указанного федерального закона отзываю у Государственного бюджетного дошкольного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга ранее данное мной согласие на обработку персональных данных. В случае, если согласие на обработку персональных данных давалось мной неоднократно, настоящим я отзываю все ранее данные мной ГБДОУ детскому саду № 6 согласия на обработку персональных данных.

Напоминаю, что, в соответствии со ст. 21 п. 5 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ, в случае отзыва субъектом персональных данных согласия на их обработку, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

Указанное уведомление прошу предоставить в письменной форме.
Дата: «____»_____ 20____г.
_____/_____
(Подпись) (фамилия, имя, отчество)

Приложение № 12
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Разъяснение субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в связи с поступлением на работу

Уважаемый(-ая),
_____!
(фамилия, имя, отчество)

В соответствии с частью 2 статьи 18 Федерального закона Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных» уведомляем Вас, что обработка персональных данных осуществляется в связи с реализацией трудовых или служебных отношений.

В связи с отказом Вами предоставить установленные законодательством Российской Федерации, нормативными правовыми актами Российской Федерации, статьёй 86 Трудового кодекса Российской Федерации персональные данные, ГБДОУ детский сад № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга не сможет реализовать с Вами трудовые или служебные отношения.

В связи с вышеизложенным представленные Вами документы будут возвращены без рассмотрения.

С уважением, _____
(должность, фамилия и инициалы)

_____
(дата)

Приложение № 13
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Уведомление об уничтожении персональных данных

Уважаемый(ая) _____,
(фамилия, имя, отчество)
в связи с _____
(причина уничтожения)
сообщаем Вам, что Ваши персональные данные уничтожены в соответствии с
_____
_____
(локальный нормативный акт, регламентирующий уничтожение персональных данных)

_____/_____/_____
(должность) (фамилия, инициалы) (подпись)
«____»_____20___г.

Приложение № 14
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6
УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Дополнительное соглашение №___
к договору №____ от _____20___года

Санкт-Петербург «___»_____20____г.

Государственное бюджетное дошкольное образовательное учреждение детский сад №6 общеразвивающего вида Кронштадтского района Санкт-Петербурга (далее – образовательная организация) осуществляющая образовательную деятельность на основании лицензии от «15» мая 2012 года N 78 №02261, выданной Комитетом по образованию Санкт-Петербурга, именуемое в дальнейшем «Работодатель», в лице заведующего ГБДОУ №6 Кияниченко Елены Евгеньевны, действующей на основании Устава, и

_____
(фамилия, имя, отчество (при наличии)/ наименование юридического лица)
именуем___ в дальнейшем «Работник», паспорт серии _____№_____, выдан:
_____
_____
(место и дата выдачи паспорта)
заключили настоящее дополнительное соглашение к договору №_____ от _____года о нижеследующем:

1. Глава VII договора №_____ от _____года изложить в следующей редакции:
2. Основание для изменения – _____
(указывается документ, в котором отражены изменения персональных данных)
Копия прилагается.
3. Остальные пункты остаются в договоре без изменений.

Настоящее дополнительное соглашение является неотъемлемой частью договора №_____ от _____20____года, действует с «___»_____20____ года и составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из сторон.

Работодатель
Государственное бюджетное дошкольное образовательное учреждение детский сад №6 общеразвивающего вида Кронштадтского района Санкт-Петербурга
ИНН: 7818011037
Адрес: 197760, Санкт-Петербург, г.Кронштадт, ул. Флотская, д.10а
Тел. 311-37-62, 311-13-70

Заведующий ГБДОУ детского сада №6
_____Е.Е.Кияниченко

М.П.

Работник
ФИО полностью_____
_____
Паспортные данные: серия _____
№_____, кем и когда выдан:
_____
_____
_____
Адрес регистрации: _____
_____

_____/_____
Подпись Расшифровка
«_____»_____20_____года

Один экземпляр дополнительного соглашения получил: _____
(дата)
_____
(подпись) (расшифровка)

Приложение № 15
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Перечень сведений конфиденциального характера (информации, доступ к которой ограничен в соответствии с федеральными законами), подлежащих защите.

Содержание сведений	Основание для включения в перечень
Сведения о частной жизни лиц, за исключением сведений, подлежащих распространению в установленных федеральными законами случаях и предоставленных для опубликования в открытой печати.	Ст. 24 Конституции Российской Федерации
Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.	Указ Президента Российской Федерации "Об утверждении перечня сведений конфиденциального характера" от 06.03.1997 № 188
Сведения о частной жизни лица, составляющие его личную или семейную тайну.	Ст. 137 Уголовного кодекса Российской Федерации
Сведения, затрагивающие частную жизнь, честь и достоинство граждан.	Ст. 4 Федерального закона от 21.07.1997
Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности.	Ст. 9 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации"
Информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника: личные сведения о работнике, данные об образовании, квалификации, трудовом стаже, состоянии здоровья, персонифицированные сведения, сведения, необходимые для ведения воинского учета.	Ст. 65, 85 Трудового Кодекса Российской Федерации
Любая информация, относящаяся прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).	Ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных"

СОГЛАСОВАНО:

Заведующий ГБДОУ
Детского сада № 6 _____/ Е.Е. Кияниченко

Приложение № 16
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Перечень информационных систем персональных данных ГБДОУ детского сада № 6 Кронштадтского района Санкт-Петербурга

№	**Информационная система**	**Размещаемые данные**
1.	«Параграф»	данные работников (личные дела), данные воспитанников (личные дела) и их родителей (законных представителей)
2.	«АРГОС»	данные работников
3.	«Электронный детский сад»	данные воспитанников и их родителей (законных представителей)

Согласовано:

Заведующий ГБДОУ
Детского сада № 6 _____/Кияниченко Е.Е.

Приложение № 17
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Частная модель угроз безопасности персональных данных для информационной системы персональных данных Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга

В настоящем документе используются следующие термины и их определения:

Аутентификация отправителя данных - подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) - исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения.

Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа - программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) - получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации - возможность получения информации и ее использования.

Закладочное устройство - элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал - электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПД) - информационная система,

представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных - обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран - локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных - физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор (персональных данных) - муниципальный орган, юридическое лицо, организующее и осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПД (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической,

видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) - неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» - комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных - умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных - действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду

до технического средства, осуществляющего перехват информации.

Уязвимость - слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации - способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Принятые сокращения:

ВТСС – вспомогательные технические средства и системы
ИБ – информационная безопасность
ИСПД – информационная система персональных данных
НСД – несанкционированный доступ
ПД – персональные данные
ПО – программное обеспечение
ПЭВМ – персональная электронно-вычислительная машина
ПЭМИН – побочные электромагнитные излучения и наводки
ПСЗИ – программные средства защиты информации
СВТ – средства вычислительной техники
СЗИ – средства защиты информации
СЗПД – средства защиты персональных данных
СКЗИ – средства криптографической защиты информации
СФ СЗПД – среда функционирования средств защиты персональных данных
УБПД – угроза безопасности персональных данных

ВВЕДЕНИЕ

В настоящем документе представлена Модель угроз безопасности персональных данных (далее – Модель угроз) и модель нарушителя информационной системы персональных данных (далее – ИСПД) автоматизированной системы Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга (далее – ГБДОУ № 6).

Модель угроз разработана в соответствии со следующими основными документами:

– Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Постановление 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 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.);

– Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.).

Модель угроз может быть пересмотрена:

– по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

– по результатам мероприятий по контролю за выполнением требований к обеспечению

безопасности персональных данных при их обработке в информационной системе.

Модель угроз базируется на следующих принципах:

1) Безопасность персональных данных при их обработке в ИСПД обеспечивается с помощью системы защиты персональных данных (СЗПД).

2) При формировании модели угроз учитываются как угрозы, осуществление которых нарушает безопасность персональных данных (далее - прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее - косвенные угрозы) или косвенных угроз.

3) Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

4) Система защиты персональных данных не может обеспечить защиту информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗПД не может обеспечить защиту информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

1. НАЗНАЧЕНИЕ, СТРУКТУРА И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИСПД

1.1. ИСПД предназначена для выполнения в электронном виде следующих основных процедур:

– формирование базы персональных данных воспитанников ГБДОУ № 6, включающих ПД воспитанников и их родителей;

– формирование базы персональных данных работников ГБДОУ № 6;

Расчетный объем обрабатываемых персональных данных: менее 1000 субъектов персональных данных.

ИСПД не относится к:

– информационной системе, обрабатывающей специальные категории персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных;

– информационной системе, обрабатывающей биометрические персональные данные, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных;

– информационной системе, обрабатывающей общедоступные персональные данные, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных».

ИСПД подключена к информационно-телекоммуникационной сети «Интернет».

Режим обработки персональных данных: многопользовательский.

Режим разграничения прав доступа пользователей информационной системы: с разграниченными правами доступа.

Местонахождение ИСПД: Российская Федерация, город Санкт-Петербург, город Кронштадт, Флотская ул., д.10а

2. ОПИСАНИЕ ФОРМ ПРЕДСТАВЛЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Персональные данные имеют различные формы представления (носители ПД) с учетом используемых в информационной системе информационных технологий и технических средств.

Носитель ПД - материальный объект, в том числе физическое поле, в котором ПД находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Носители ПД содержат информацию, в следующих видах:

– видовая информация, представленная в виде текста и изображений различных устройств отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средства обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПД;
– информация, обрабатываемая (циркулирующая) в ИСПД, в виде электрических, электромагнитных, оптических сигналов;
– информация, обрабатываемая в ИСПД, представленная в виде бит, байт, IP- протоколов, файлов и других логических структур.

3. ОПРЕДЕЛЕНИЕ ХРАКТЕРИСТИК БЕЗОПАСНОСТИ

Основными характеристиками безопасности являются конфиденциальность, целостность и доступность.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Доступность информации - состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

4. МАТРИЦА ДОСТУПА

Матрица доступа отражает права всех групп субъектов доступа ИСПД на действия с персональными данными. Действия (операции) с персональными данными, включают сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных).

Матрица доступа для ИСПД представлена в таблице 1

Таблица 1

Группа	**Уровень доступа к персональным данным**	**Разрешенные действия**
Администратор ИСПД	- Обладает полной информацией о системном и прикладном программном обеспечении ИСПД. - Обладает полной информацией о технических средствах и конфигурации ИСПД. - Имеет доступ ко всем техническим средствам обработки информации и данным ИСПД. - Обладает правами конфигурирования и административной настройки технических средств ИСПД.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение - распространение - блокирование - обезличивание
Администратор безопасности	- Обладает правами Администратора ИСПД. - Обладает полной информацией об ИСПД. - Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПД. - Не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).	- сбор, -систематизация - накопление - хранение,- уточнение - использование - уничтожение - распространение - блокирование - обезличивание

Оператор ИСПД	Обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ ко всем персональным данным.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение

5. УРОВЕНЬ ИСХОДНОЙ ЗАЩИЩЕННОСТИ

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПД (Y1), приведенных в таблице 1.

Таблица 1

Технические и эксплуатационные характеристики ИСПД	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
распределённая ИСПД, которая охватывает несколько областей, краев, округов или государство в целом;			+
городская ИСПД, охватывающая не более одного населенного пункта (города, поселка);			+
корпоративная распределенная ИСПД, охватывающая многие подразделения одной организации;		+	
локальная (кампусная) ИСПД, развернутая в пределах нескольких близко расположенных зданий;		+	
локальная ИСПД, развернутая в пределах одного здания.	+		
2. По наличию соединения с сетями общего пользования:			
ИСПД, имеющая многоточечный выход в сеть общего пользования;			+
ИСПД, имеющая одноточечный выход в сеть общего пользования;		+	
ИСПД, физически отделенная от сети общего пользования.	+		
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+		
запись, удаление, сортировка;		+	
модификация, передача.			+
4. По разграничению доступа к персональным данным:			
ИСПД, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПД, либо субъект ПД;		+	
ИСПД, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПД;			+
ИСПД с открытым доступом.			+
5. По наличию соединений с другими базами ПД иных ИСПД:			
интегрированная ИСПД (организация использует несколько баз ПД ИСПД, при этом организация не является владельцем всех используемых баз ПД);			+
ИСПД, в которой используется одна база ПД, принадлежащая организации-владельцу данной ИСПД.	+		
6. По уровню обезличивания ПД:			
ИСПД в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+		

ИСПД, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;		+	
ИСПД, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПД).			+
7. По объему ПД, которые предоставляются сторонним пользователям ИСПД без предварительной обработки:			
ИСПД, предоставляющая всю БД с ПД;			+
ИСПД, предоставляющая часть ПД;		+	
ИСПД, не предоставляющие никакой информации.	+		

Исходная степень защищенности определяется следующим образом:

1) ИСПД имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПД соответствуют уровню "высокий" (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные - среднему уровню защищенности (положительные решения по второму столбцу) (Yi= 0).

2) ИСПД имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПД соответствуют уровню не ниже "средний" (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности (Yi= 5).

3) ИСПД имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2 (Yi= 10).

Технические и эксплуатационные характеристики	ИСПД
По территориальному размещению	средний
По наличию соединения с сетями общего пользования	средний
По встроенным (легальным) операциям с записями баз персональных данных	средний
По разграничению доступа к персональным данным	средний
По наличию соединений с другими базами ПД иных ИСПД	высокий
По уровню обезличивания ПД	средний
По объему ПД, которые предоставляются сторонним пользователям ИСПД без предварительной обработки	средний
Уровень защищенности	средний
Значение Y1	5

ИСПД ГБДОУ № 6 присвоен средний уровень исходной защищенности.

Одновременно с этим по таблице определения уровня защищенности в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 присваивается 3 уровень защищенности ИСПД.

6. ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ

6.1. Состав и содержание УБПД определяется совокупностью условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПД обрабатываемым в ИСПД.

Основными элементами ИСПД являются:

– персональные данные, обрабатываемые в ИСПД;

– информационные технологии, как совокупность приемов, способов и методов применения средств вычислительной техники при обработке ПД;

– технические средства ИСПД, осуществляющие обработку ПД (средства вычислительной техники (СВТ), информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПД;

– программные средства (операционные системы, системы управления базами данных и т.п.);
– средства защиты информации (СЗИ), включая СКЗИ;
– вспомогательные технические средства и системы (технические средства и системы, их коммуникации, не предназначенные для обработки ПД, но размещенные в помещениях, в которых расположены ИСПД, такие как средства вычислительной техники, средства и системы охранной и пожарной сигнализации, средства и системы кондиционирования, средства электронной оргтехники и т.п.) (далее - ВТСС);
– документация на СКЗИ и на технические и программные компоненты ИСПД;
– ключевая, аутентифицирующая и парольная информация;
– помещения, в которых находятся защищаемые ресурсы.

Возможности источников УБПД обусловлены совокупностью методов и способов несанкционированного и (или) случайного доступа к ПД, в результате которого возможно нарушение конфиденциальности (копирование, неправомерное распространение), целостности (уничтожение, изменение) и доступности (блокирование) ПД.

Угроза безопасности ПД реализуется в результате образования канала реализации УБПД между источником угрозы и носителем (источником) ПД, что создает необходимые условия для нарушения безопасности ПД (несанкционированный или случайный доступ).

Основными элементами канала реализации УБПД являются:

– источник УБПД - субъект, материальный объект или физическое явление, создающие УБПД;
– среда (путь) распространения ПД или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, целостность, доступность) ПД;
– носитель ПД - физическое лицо или материальный объект, в том числе физическое поле, в котором ПД находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Источниками угроз НСД в ИСПД могут быть:

– нарушитель;
– носитель вредоносной программы.

6.2. КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ

По признаку принадлежности к ИСПД все нарушители делятся на две группы:

– внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПД;
– внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПД.

6.2.1. ВНЕШНИЙ НАРУШИТЕЛЬ

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПД, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

6.2.2. ВНУТРЕННИЙ НАРУШИТЕЛЬ

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно-технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированного доступа.

Система разграничения доступа ИСПД обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам ИСПД в

соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

– администратор базы данных ИСПД (категория I);
– администраторы оператора ИСПД (категория II);
– сотрудники оператор ИСПД (категория III);
– заявители ИСПД (категория IV);
– лица, обладающие возможностью доступа к системе передачи данных (категория V);
– сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются элементы ИСПД, но не имеющие права доступа к ним (категория VI);
– обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) (категория VII);
– уполномоченный персонал разработчиков ИСПД, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПД (категория VIII).

На лиц категорий I и II возложены задачи по администрированию программно-аппаратных средств и баз данных ИСПД для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПД. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПД, а также к техническим и программным средствам ИСПД в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПД в целом, а также с применяемыми принципами и концепциями безопасности.

Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

К лицам категорий I и II ввиду их исключительной роли в ИСПД должен применяться комплекс особых организационно-режимных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей. Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III-VIII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

7. ПРЕДПОЛОЖЕНИЯ ОБ ИМЕЮЩЕЙСЯ У НАРУШИТЕЛЯ ИНФОРМАЦИИ ОБ ОБЪЕКТАХ РЕАЛИЗАЦИИ УГОРОЗ

В качестве основных уровней знаний нарушителей об ИСПД можно выделить следующие:

– *общая информация* - информации о назначении и общих характеристиках ИСПД;
– *эксплуатационная информация* - информация, полученная из эксплуатационной документации;
– *чувствительная информация* - информация, дополняющая эксплуатационную информацию об ИСПД (например, сведения из проектной документации ИСПД).

В частности, нарушитель может иметь:

– данные об организации работы, структуре и используемых технических, программных и программно-технических средствах ИСПД;
– сведения об информационных ресурсах ИСПД: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
– данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно - технических средств ИСПД;
– данные о реализованных в ПСЗИ принципах и алгоритмах;

– исходные тексты программного обеспечения ИСПД;
– сведения о возможных каналах реализации угроз;
– информацию о способах реализации угроз.

Предполагается, что лица категории III и категории IV владеют только эксплуатационной информацией, что обеспечивается организационными мерами. При этом лица категории IV не владеют парольной, аутентифицирующей и ключевой информацией, используемой в ИСПД, к которым они не имеют санкционированного доступа.

Предполагается, что лица категории V владеют в той или иной части чувствительной и эксплуатационной информацией о системе передачи информации и общей информацией об ИСПД, использующих эту систему передачи информации, что обеспечивается организационными мерами. При этом лица категории V не владеют парольной и аутентифицирующей информацией, используемой в ИСПД.

Предполагается, что лица категории VI и лица категории VII по уровню знаний не превосходят лица категории V.

Предполагается, что лица категории VIII обладают чувствительной информацией об ИСПД, включая информацию об уязвимостях технических и программных средств ИСПД. Организационными мерами предполагается исключить доступ лиц категории VIII к техническим и программным средствам ИСПД в момент обработки с использованием этих средств защищаемой информации.

Таким образом, наиболее информированными об ИСПД являются лица категории III и лица категории VIII.

Степень информированности нарушителя зависит от многих факторов, включая организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания определенного запаса прочности предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

8. ПРЕДПОЛОЖЕНИЯ ОБ ИМЕЮЩИХСЯ У НАРУШИТЕЛЯ СРЕДСТВАХ РЕАЛИЗАЦИИ УГРОЗ

Предполагается, что нарушитель имеет:
– аппаратные компоненты СЗПД и СФ СЗПД;
– доступные в свободной продаже технические средства и программное обеспечение;
– специально разработанные технические средства и программное обеспечение.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объектах ГБДОУ № 6 конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для создания устойчивой СЗПД предполагается, что вероятный нарушитель имеет все необходимые для реализации угроз средства, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:
– средств перехвата в технических каналах утечки;
– средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы технических средств, входящих в состав ИСПД);
– средств воздействия на источники и через цепи питания;
– средств воздействия через цепи заземления;
– средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории III и лица категории VIII.

9. КЛАССИФИКАЦИЯ УЯЗВИМОСТЕЙ ИСПД

Уязвимость ИСПД - недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении автоматизированной информационной системы, которое может быть использовано для реализации угрозы безопасности персональных данным.

Причинами возникновения уязвимостей являются:

– ошибки при проектировании и разработке программного (программно-аппаратного) обеспечения;

– преднамеренные действия по внесению уязвимостей в ходе проектирования и разработки программного (программно-аппаратного) обеспечения;

– неправильные настройки программного обеспечения, неправомерное изменение режимов работы устройств и программ;

– несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);

– внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;

– несанкционированные неумышленные действия пользователей, приводящие к возникновению уязвимостей;

– сбои в работе аппаратного и программного обеспечения (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Различают следующие группы основных уязвимостей:

– уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);

– уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

10. ПЕРЕЧЕНЬ ВОЗМОЖНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для ИСПД можно выделить следующие угрозы:

1. Угрозы от утечки по техническим каналам.

1.1. У грозы утечки акустической информации.

1.2. Угрозы утечки видовой информации.

1.3. У грозы утечки информации по каналам ПЭМИН.

2. Угрозы несанкционированного доступа к информации.

2.1. Угрозы уничтожения, хищения аппаратных средств ИСПД носителей информации путем физического доступа к элементам ИСПД.

2.1.1. Кража технических средств входящих в состав ИСПД;

2.1.2. Кража носителей информации;

2.1.3. Кража ключей и атрибутов доступа;

2.1.4. Кражи, модификации, уничтожения информации;

2.1.5. Вывод из строя узлов технических средств, входящих в состав ИСПД, каналов связи;

2.1.6. Несанкционированное отключение средств защиты.

2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

2.2.1. Действия вредоносных программ (вирусов);

2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных;

2.2.3. Установка ПО не связанного с исполнением служебных обязанностей.

2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПД и СЗПД в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.
2.3.1. Утрата ключей и атрибутов доступа;
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками;
2.3.3. Непреднамеренное отключение средств защиты;
2.3.4. Выход из строя аппаратно-программных средств;
2.3.5. Сбой системы электроснабжения;
2.3.6. Стихийное бедствие.
2.4. Угрозы преднамеренных действий внутренних нарушителей.
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке;
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.
2.5. Угрозы несанкционированного доступа по каналам связи.
2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПД и принимаемой из внешних сетей информации:
2.5.1.1. Перехват за переделами с контролируемой зоны;
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.
2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПД, топологии сети, открытых портов и служб, открытых соединений и др.
2.5.3. Угрозы выявления паролей по сети.
2.5.4. Угрозы навязывание ложного маршрута сети.
2.5.5. Угрозы подмены доверенного объекта в сети.
2.5.6. Угрозы внедрения ложного объекта как в ИСПД, так и во внешних сетях.
2.5.7. Угрозы типа «Отказ в обслуживании».
2.5.8. Угрозы удаленного запуска приложений.
2.5.9. Угрозы внедрения по сети вредоносных программ.

11. ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГОРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПД для ИСПД в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

– маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

– низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

– средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПД недостаточны (Y2 = 5);

– высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПД не приняты (Y2 = 10).

Определение вероятности реализации угрозы, должно быть проведено для всех выявленных угроз. Ниже приведено описание каждой угрозы и даны обобщенные вероятности реализации угроз для каждого типа ИСПД.

11.1. Угрозы утечки информации по техническим каналам.

11.1.1. Угрозы утечки акустической (речевой) информации.

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПД, при обработке ПД в ИСПД, возможно при наличием функций голосового ввода ПД в ИСПД или функций воспроизведения ПД акустическими средствами ИСПД.

В ИСПД функции голосового ввода ПД или функции воспроизведения ПД акустическими средствами отсутствуют. Поэтому для всех типов ИСПД вероятность реализации угрозы - **являются маловероятными**.

11.1.2. Угрозы утечки видовой информации.

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико-электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПД.

При условии, что в здании Оператора, где размещена ИСПД введен контроль доступа в контролируемую зону, а рабочие места пользователей расположены так, что практически исключен визуальный доступ к мониторам, то для ИСПД вероятность реализации рассматриваемой угрозы - **является маловероятной**.

11.1.3. Угрозы утечки информации по каналам ПЭМИН.

Угрозы утечки информации по каналу ПЭМИН, возможны из-за наличия паразитных электромагнитных излучений у элементов ИСПД.

Угрозы данного класса **маловероятны** для ИСПД, т.к. размер контролируемой зоны большой, и элементы ИСПД, находятся в самом центре здания и экранируются несколькими несущими стенами, и паразитный сигнал маскируется со множеством других паразитных сигналов элементов не входящих в ИСПД.

11.2. Угрозы несанкционированного доступа к информации.

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

11.2.1. Угрозы уничтожения, хищения аппаратных средств ИСПД носителей информации путем физического доступа к элементам ИСПД

11.2.1.1. Кража технических средств, входящих в состав ИСПД.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПД.

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, двери закрываются на замок, то вероятность реализации данной угрозы - **является маловероятной**.

11.2.1.2. Кража носителей информации.

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, двери закрываются на замок, ведется учет и хранение носителей, то вероятность реализации данной угрозы - **является маловероятной**.

11.2.1.3. Кража ключей и атрибутов доступа.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, двери закрываются на замок, организовано хранение ключей и введена политика «чистого стола», то вероятность реализации данной угрозы - **является маловероятной**.

11.2.1.4. Кража, модификация, уничтожение информации.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПД и средства защиты, а так же происходит работа пользователей.

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, двери закрываются на замок, то вероятность реализации данной угрозы - **является маловероятной**.

11.2.1.5. Вывод из строя узлов технических средств, входящих в состав ИСПД, каналов связи.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПД и проходят каналы связи.

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, двери закрываются на замок, то вероятность реализации данной угрозы - **является маловероятной**.

11.2.1.6. Несанкционированное отключение средств защиты.

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПД.

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, двери закрываются на замок, пользователи ИСПД проинструктированы о работе с персональными данными, то вероятность реализации данной угрозы - **является маловероятной**.

11.2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).

11.2.2.1. Действия вредоносных программ (вирусов).

Программно-математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать признаки своего присутствия в программной среде компьютера;

– обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

У Оператора на всех элементах ИСПД установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения, таким образом вероятность реализации угрозы - **является низкой.**

11.2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных.

Недекларированные возможности - функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Вероятность реализации угрозы повышается:

– при увеличении элементов, в том числе программного обеспечения, ИСПД;

– при увеличении числа функциональных связей между элементами;

– наличии подключения к сетям общего доступа и (или) международного обмена.

Для рассматриваемой ИСПД вероятность реализации угрозы - **низкая.**

11.2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПД или ее элементов.

У Оператора введено разграничение правами пользователей на установку ПО и осуществляется контроль, пользователи проинструктированы о политике установки ПО,

таким образом для рассматриваемой ИСПД вероятность реализации угрозы - **является маловероятной**.

11.2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПД и СЗПД в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

11.2.3.1. Утрата ключей и атрибутов доступа.

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПД, которые нарушают положения парольной политики в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

У Оператора введена парольная политика, предусматривающая требуемую сложность пароля и периодическую его смену, введена политика «чистого стола», осуществляется контроль за их выполнением, пользователи проинструктированы о парольной политике и о действиях в случаях утраты или компрометации паролей, таким образом для рассматриваемой ИСПД вероятность реализации угрозы - **является низкой**.

11.2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками.

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПД, которые нарушают положения принятых правил работы с ИСПД или не осведомлены о них.

Принимая во внимание, что в ИСПД осуществляется резервное копирование обрабатываемых ПД, пользователи проинструктированы о работе с ИСПД, то для рассматриваемой ИСПД вероятность реализации угрозы - **является низкой, так как нельзя полностью исключать человеческий фактор**.

11.2.3.3. Непреднамеренное отключение средств защиты.

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПД, которые нарушают положения принятых правил работы с ИСПД и средствами защиты или не осведомлены о них.

Принимая во внимание, что у Оператора введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПД, то вероятность реализации угрозы - **является маловероятной**.

11.2.3.4. Выход из строя аппаратно-программных средств.

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

У Оператора осуществляет резервирование ключевых элементов ИСПД, таким образом для рассматриваемой ИСПД вероятность реализации угрозы - **является маловероятной**.

11.2.3.5. Сбой системы электроснабжения.

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

У Оператора ко всем ключевым элементам ИСПД осуществляет резервное копирование информации, таким образом для рассматриваемой ИСПД вероятность реализации угрозы - **является маловероятной**.

11.2.3.6. Стихийное бедствие.

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

У Оператора установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций, таким образом для рассматриваемой ИСПД вероятность реализации угрозы – **является маловероятной**.

11.2.4. Угрозы преднамеренных действий внутренних нарушителей.

11.2.4.1. Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке.

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПД и средства защиты, а так же происходит работа пользователей.

У Оператора введен контроль доступа в контролируемую зону, двери закрываются на замок. При наличии вышеперечисленных мер вероятность реализации угрозы - **является маловероятной**

11.2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке.

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПД, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

У Оператора пользователи осведомлены о порядке работы с персональными данными, а так же подписали Договор о неразглашении, то для рассматриваемой ИСПД вероятность реализации угрозы - **является низкой**.

При неосведомленности пользователей и не заключении Договора о неразглашении, вероятность реализации угрозы должна быть пересмотрена или необходимо принять меры к снижению вероятности реализации угрозы.

11.2.5. Угрозы несанкционированного доступа по каналам связи.

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПД, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПД можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

11.2.5.1. Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПД и принимаемой из внешних сетей информации;

11.2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПД, топологии сети, открытых портов и служб, открытых соединений и др.;

11.2.5.3. Угрозы выявления паролей по сети;

11.2.5.4. Угрозы навязывания ложного маршрута сети;

11.2.5.5. Угрозы подмены доверенного объекта в сети;

11.2.5.6. Угрозы внедрения ложного объекта как в ИСПД, так и во внешних сетях;

11.2.5.7. Угрозы типа «Отказ в обслуживании»;

11.2.5.8. Угрозы удаленного запуска приложений;

11.2.5.9. Угрозы внедрения по сети вредоносных программ.

Принимая во внимание, что формирование личных дел воспитанников и работников ГБДОУ № 6 осуществляется не только на основании исключительно автоматизированной обработки персональных данных в отношении субъекта персональных данных, то для рассматриваемой ИСПД вероятность реализации вышеперечисленных угроз - **является маловероятной**.

Актуальность угроз в зависимости от их реализуемости и опасности

Тип угроз безопасности ПД	Реализуемость угрозы (Y1+Y2) / 20	Опасность угрозы	Актуальность угрозы
1. Угрозы утечки информации по техническим каналам.			
1.1. Угрозы утечки акустической информации.	0,25 низкая	средняя	неактуальная
1.2. Угрозы утечки видовой информации.	0,25 низкая	средняя	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН.	0,25 низкая	средняя	неактуальная
2. Угрозы несанкционированного доступа к информации.			
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПД носителей информации путем физического доступа к элементам ИСПД.			
2.1.1.Кража технических средств, входящих в состав ИСПД.	0,25 низкая	средняя	неактуальная

2.1.2. Кража носителей информации.	0,25 низкая	средняя	неактуальная
2.1.3. Кража ключей и атрибутов доступа.	0,25 низкая	средняя	неактуальная
2.1.4. Кражи, модификации, уничтожения информации.	0,25 низкая	средняя	неактуальная
2.1.5. Вывод из строя узлов технических средств, входящих в состав ИСПД, каналов связи.	0,25 низкая	средняя	неактуальная
2.1.6. Несанкционированное отключение средств защиты.	0,25 низкая	средняя	неактуальная
2.1.7. Несанкционированное отключение средств защиты.	0,25 низкая	средняя	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).			
2.2.1. Действия вредоносных программ (вирусов).	0,35 средняя	средняя	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных.	0,35 средняя	средняя	актуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей.	0,25 низкая	средняя	неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПД и СЗПД в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.			
2.3.1. Утрата ключей и атрибутов доступа.	0,35 средняя	средняя	актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками.	0,35 средняя	средняя	актуальная
2.3.3. Непреднамеренное отключение средств защиты.	0,25 низкая	средняя	неактуальная
2.3.4. Выход из строя аппаратно-программных средств.	0,25 низкая	средняя	неактуальная
2.3.5. Сбой системы электроснабжения.	0,25 низкая	средняя	неактуальная
2.3.6. Стихийное бедствие.	0,25 низкая	средняя	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей.			
2.4.1. Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке.	0,25 низкая	средняя	неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.	0,35 средняя	средняя	актуальная
2.5.Угрозы несанкционированного доступа по каналам связи.			
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПД и принимаемой из внешних сетей информации.	0,25 низкая	средняя	неактуальная

2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПД, топологии сети, открытых портов и служб, открытых соединений и др.	0,25 низкая	средняя	неактуальная
2.5.3.Угрозы выявления паролей по сети.	0,25 низкая	средняя	неактуальная
2.5.4.Угрозы навязывания ложного	0,25 низкая	средняя	неактуальная
2.5.5.Угрозы подмены доверенного объекта в сети.	0,25 низкая	средняя	неактуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПД, так и во внешних сетях.	0,25 низкая	средняя	неактуальная
2.5.7.Угрозы типа «Отказ в обслуживании».	0,25 низкая	средняя	неактуальная
2.5.8.Угрозы удаленного запуска приложений.	0,25 низкая	средняя	неактуальная
2.5.9.Угрозы внедрения по сети вредоносных программ.	0,35 средняя	средняя	актуальная

Рекомендуемыми мерами по предотвращению реализации актуальных угроз, являются:

− своевременное обновление антивирусной защиты;

− использование протокола защищенного соединение (HTTPS);

− парольная политика, устанавливающая обязательную сложность и периодичность смены пароля;

− инструкции пользователей ИСПД, в которых отражены порядок безопасной работы с ИСПД, а так же с ключами и атрибутами доступа;

− осуществление резервирования ключевых элементов ИСПД;

− организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПД и средств защиты.

Приложение № 18
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Мероприятия по безопасности персональных данных в Государственном бюджетном дошкольном образовательном учреждении детском саду № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга

1. Разработать положение о защите персональных данных воспитанников ГБДОУ детского сада № 6.
2. Разработать положение о защите персональных данных работников ГБДОУ детского сада № 6.
3. Составить перечень сведений конфиденциального характера, подлежащих защите.
4. Составить перечень информационных систем персональных данных ГБДОУ детского сада № 6.
5. Разработать положение о разграничении прав доступа к обрабатываемым персональным данным.
6. Разработать должностную инструкцию ответственного лица по организации обработки и защиты персональных данных работников, воспитанников и родителей (законных представителей) воспитанников ГБДОУ детского сада №6.
7. Составить обязательство работника о неразглашении персональных данных субъекта.
8. Обязательство о конфиденциальности и неразглашении персональных данных, ставших известными работнику, осуществляющему обработку персональных данных, в случае расторжения с ним трудовых отношений.
9. Разработать политику Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 Кронштадтского района Санкт-Петербурга в отношении обработки персональных данных.
10. Разработать положение об ответственности работников, допущенных к обработке персональных данных и иной конфиденциальной информации ГБДОУ детского сада № 6 Кронштадтского района Санкт-Петербурга.
11. Разработать новую форму согласия на обработку персональных данных несовершеннолетних и согласие на обработку персональных данных с учетом требований законодательства РФ.
12. Разработать модель угроз для информационной системы ГБДОУ детского сада № 6.
13. Утвердить форму журнала регистрации выявленных нарушений.
14. Утвердить порядок учета и использования машинных носителей информации, содержащих персональные данные и иную конфиденциальную информацию.
15. Утвердить журнал учета машинных носителей информации.
16. Разработать правила рассмотрения запросов субъектов персональных данных или их представителей в Государственном бюджетном дошкольном образовательном учреждение детском саду № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга.
17. Разработать положение о персональных данных.
18. Утвердить порядок уничтожения, блокирования персональных данных.
19. Определить места хранения персональных данных и границы зоны контроля.
20. Усовершенствовать средства физической охраны персональных данных.
21. Своевременно обновлять технические средства защиты персональных данных.

Приложение № 19
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Акт № 1 классификации информационной системы персональных данных «Параграф» Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга

Комиссия, назначенная приказом Заведующего ГБДОУ № 6 от «03» сентября 2018 года № 56/1-Д «О разработке пакета документов по безопасности персональных данных в ГБДОУ детском саду № 6 Кронштадтского района Санкт-Петербурга»
в составе:

председатель комиссии:
Заведующий ГБДОУ детского сада № 6 Е.Е.Кияниченко
члены комиссии:
Заместитель заведующего ГБДОУ № 6 А.В.Хилюк
Ответственный за безопасность персональных данных Е.В.Федорова

провела обследование информационной системы «Параграф» и обрабатываемых в ней персональных данных в целях её классификации.

По результатам проведенного обследования комиссия установила:

1. Категория обрабатываемых персональных данных – иные персональные данные.
2. Категория субъектов персональных данных – работники ГБДОУ №6, воспитанники ГБДОУ № 6 и их родители (законные представители)
3. Количество субъектов обрабатываемых персональных данных – менее 1000 человек.
4. Тип актуальных угроз – угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении.
5. Уровень значимости информации – средний.
6. Масштаб информационной системы – объектовый.

В соответствии с Моделью угроз безопасности персональных данных при их обработке в Государственном бюджетном дошкольном образовательном учреждение детском саду № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга и требованиями постановления Правительства Российской Федерации от «01» ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», информационной системе присвоен уровень защищенности **- 3** (УЗ-3).

В соответствии с Приказом ФСТЭК России от «11» февраля 2013 г. №17 «Об утверждении требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», учитывая установленный уровень защищенности персональных данных, информационной системе присвоен класс защищенности **- 3** (К3).

Председатель комиссии:
Заведующий ГБДОУ детского сада № 6 _____/Е.Е.Кияниченко

Члены комиссии:
Заместитель заведующего ГБДОУ № 6 _____/А.В.Хилюк
Ответственный за безопасность персональных данных _____/Е.В.Федорова

Акт № 2 классификации информационной системы персональных данных «АРГОС» Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга

Комиссия, назначенная приказом Заведующего ГБДОУ № 6 от «03» сентября 2018 года № 56/1-Д «О разработке пакета документов по безопасности персональных данных в ГБДОУ детском саду № 6 Кронштадтского района Санкт-Петербурга»
в составе:

председатель комиссии:

Заведующий ГБДОУ детского сада № 6 Е.Е.Кияниченко

члены комиссии:

Заместитель заведующего ГБДОУ № 6 А.В.Хилюк

Ответственный за безопасность персональных данных Е.В.Федорова

провела обследование информационной системы «АРГОС» и обрабатываемых в ней персональных данных в целях её классификации.

По результатам проведенного обследования комиссия установила:

1. Категория обрабатываемых персональных данных – иные персональные данные.
2. Категория субъектов персональных данных – работники ГБДОУ №6
3. Количество субъектов обрабатываемых персональных данных – менее 1000 человек.
4. Тип актуальных угроз – угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении.
5. Уровень значимости информации – средний.
6. Масштаб информационной системы – объектовый.

В соответствии с Моделью угроз безопасности персональных данных при их обработке в Государственном бюджетном дошкольном образовательном учреждение детском саду № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга и требованиями постановления Правительства Российской Федерации от 01 ноября 2012 г. NQ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», информационной системе присвоен уровень защищенности **- 3** (УЗ-3).

В соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. N2 17 «Об утверждении требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», учитывая установленный уровень защищенности персональных данных, информационной системе присвоен класс защищенности **- 3** (К3).

Председатель комиссии:
Заведующий ГБДОУ детского сада № 6 _____/Е.Е.Кияниченко

Члены комиссии:
Заместитель заведующего ГБДОУ № 6 _____/А.В.Хилюк
Ответственный за безопасность персональных данных _____/Е.В.Федорова

Акт № 3 классификации информационной системы персональных данных «Электронный детский сад» Государственного бюджетного дошкольного образовательного учреждения детского сада № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга

Комиссия, назначенная приказом Заведующего ГБДОУ № 6 от «21» марта 2019 года № 26/1-Д «Об обследовании информационной системы «Электронный детский сад» и обрабатываемых в ней персональных данных в целях её классификации»
в составе:

председатель комиссии:

Заведующий ГБДОУ детского сада № 6 Е.Е.Кияниченко

члены комиссии:

Заместитель заведующего ГБДОУ № 6 А.В.Хилюк

Ответственный за безопасность персональных данных Е.В.Федорова

провела обследование информационной системы «Электронный детский сад» и обрабатываемых в ней персональных данных в целях её классификации.

По результатам проведенного обследования комиссия установила:

1. Категория обрабатываемых персональных данных – иные персональные данные.
2. Категория субъектов персональных данных – воспитанники ГБДОУ № 6 и их родители (законные представители)
3. Количество субъектов обрабатываемых персональных данных – менее 1000 человек.
4. Тип актуальных угроз – угрозы 3-го типа, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении.
5. Уровень значимости информации – средний.
6. Масштаб информационной системы – объектовый.

В соответствии с Моделью угроз безопасности персональных данных при их обработке в Государственном бюджетном дошкольном образовательном учреждение детском саду № 6 общеразвивающего вида Кронштадтского района Санкт-Петербурга и требованиями постановления Правительства Российской Федерации от «01» ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», информационной системе присвоен уровень защищенности **- 3** (УЗ-3).

В соответствии с Приказом ФСТЭК России от «11» февраля 2013 г. №17 «Об утверждении требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», учитывая установленный уровень защищенности персональных данных, информационной системе присвоен класс защищенности **- 3** (К3).

Председатель комиссии:
Заведующий ГБДОУ детского сада № 6 _____/Е.Е.Кияниченко

Члены комиссии:
Заместитель заведующего ГБДОУ № 6 _____/А.В.Хилюк
Ответственный за безопасность персональных данных _____/Е.В.Федорова

Приложение № 20
к Положению о порядке обработки и
обеспечении безопасности персональных данных
в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Инструкция пользователя информационных систем персональных данных (ИСПД) в Государственном бюджетном дошкольном образовательном учреждении детском саду № 6 общеразвивающего вида Кронштадтского района Санкт-Петербург

1. Общие положения

1.1. Пользователь информационных систем персональных данных (ИСПД) (далее - Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник ГБДОУ № 6, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами ГБДОУ № 6.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

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

1.7. 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;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- 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 ИСПД;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПД;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

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

2. Организация парольной защиты

2.1.Личные пароли доступа к элементам ИСПД выдаются пользователям Администратором информационной безопасности. Запрещается нецелевое использование подключения к Сети.

3. Права и ответственность пользователей ИСПД

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

3.2.Пользователи, виновные в несоблюдении Настоящей инструкции расцениваются как нарушители Федерального закона РФ 27.07.2006 г. №152- ФЗ «О персональных данных» и несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

4. Должностные обязанности

Пользователь обязан:

4.1.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.

4.2.Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

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

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

5.2.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 сомнительной репутации, содержащих нелегально распространяемое ПО и другие;
- запрещается нецелевое использование подключения к Сети.

Приложение № 21
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

АКТ №___
акта выявления нарушений в сфере защиты персональных данных и иной конфиденциальной информации

г. Кронштадт «____»_____20____ года

Настоящий акт составлен в том, что в Государственном бюджетном дошкольном образовательном учреждении детском саду №6 общеразвивающего вида Кронштадтского района Санкт-Петербурга

_____
(фамилия, имя, отчество допустившего нарушение)

_____
(должность)

допущено нарушение установленных требований в сфере защиты персональных данных и иной конфиденциальной
информации:__
_____
_____
(дата, место, содержание нарушения; требования каких нормативных документов нарушены)

Решение о мерах
наказания:____
_____

Комиссия (или уполномоченное лицо), выявившая нарушения

Председатель комиссии:
Заведующий ГБДОУ детского сада № 6 _____/Е.Е.Кияниченко

Члены комиссии:
Заместитель заведующего ГБДОУ № 6 _____/А.В.Хилюк
Ответственный за безопасность персональных данных _____/Е.В.Федорова

С актом ознакомлены:

подпись лица, допустившего нарушение: _____/_____
(расшифровка подписи)

Заведующий ГБДОУ детского сада № 6 _____/Е.Е.Кияниченко

Приложение № 22
к Положению о порядке обработки и обеспечении безопасности персональных данных в ГБДОУ №6

УТВЕРЖДЕНО
приказом №56/1-Д
от «03» сентября 2018 г.

Журнал регистрации выявленных нарушений
Государственного бюджетного дошкольного образовательного учреждения
детского сада № 6 общеразвивающего вида
Кронштадтского района Санкт-Петербурга

№ п/п	Число, месяц, год и время нарушения	Наименование подразделения, работниками которого нарушены требования безопасности	Ф.И.О. работника допустившего нарушение	Должность работника, допустившего нарушение	Характер нарушения	Источник информации о нарушении, в какой форме информация передана, дата сообщения	Принятые меры (наложенное взыскание, дата и № приказа)
1	2	3	4	5	6	7	8