ПРИЛОЖЕНИЕ №4

УТВЕРЖДЕНА
приказом заведующего
МБДОУ д/с №8 «Буратино»
от 01. 09.2017 № 158-ОД

ИНСТРУКЦИЯ
администратора информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая инструкция определяет функции, права и ответственность администратора информационных систем персональных данных (далее - администратор ИСПДн) в МБДОУ д/с №8 «Буратино» муниципального образования город-курорт Геленджик (далее – ДОУ).

1.2. Администратор ИСПДн является сотрудником ДОУ и назначается приказом заведующего МБДОУ д/с №8 «Буратино» (далее – заведующий).

1.3. Администратор ИСПДн обладает правами доступа к электронным носителям персональных данных в ДОУ.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства.

2.2. Периферийные устройства – монитор, клавиатура, компьютерная мышь, принтер, многофункциональные устройства, сканеры и т.д.

2.3. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.4. Доступ к информации – возможность получения информации и её использования.

2.5. Защита информации — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.6. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.7. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.8. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и

т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

2.9. Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

2.10. 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.

2.11. Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.12. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.13. Угрозы безопасности персональных данных (УБПДн) - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных.

2.14. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ

3.1. Вести учет (по вопросам обеспечения безопасности информации) и знать перечень установленных в ДОУ СЗИ и перечень задач, решаемых с их использованием.

3.2. Вести журнал учета эксплуатационной и технической документации СЗИ ИСПДн.

3.3. Вести журнал учета машинных носителей персональных данных.

3.4. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования (настройку и сопровождение) применяемых на АРМ специальных программных и программно-аппаратных СЗИ.

3.5. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных АРМ и серверов, осуществлять проверку работоспособности системы защиты после установки (обновления) программных средств ИСПДн.

3.6. Периодически проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).

3.7. Контролировать соответствие технического паспорта ИСПДн фактическому составу (комплектности) ИСПДн и вести учет изменений аппаратно- программной конфигурации (архив заявок, на основании которых были произведены данные изменения в ИСПДн).

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

3.10. Вести журнал учета нештатных ситуаций, фактов вскрытия и опечатывания АРМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств ИСПДн.

3.11. Проводить периодический инструктаж сотрудников у (пользователей ИСПДн) по правилам работы с используемыми средствами и системами зашиты информации.

3.12. Организовывать разграничения доступа:

3.13. Участвовать в разработке и знать перечень защищаемых информационных ресурсов.

3.14. Разрабатывать для ИСПДн решения по:

- составу доменов сети, системы доверительных отношений между ними;
- составу групп (локальных и глобальных) каждого домена;
- приписке пользователей с одинаковыми правами, статусом безопасности и характером решаемых задач к соответствующим группам;
- определению информационных связей между сегментами сети и требований к изоляции сегментов с использованием средств аппаратной безопасности сегментов;

3.15. Участвовать в разработке порядка пользования электронной почтой (определение списка абонентов из состава пользователей сети, проектированию системы почтовых ящиков, использованию СЗИ при передаче закрытых документов).

3.16 Участвовать в определении режимов использования СЗИ: защита паролей, защита в протоколах передачи данных, кодирование файлов, подключение дополнительных алгоритмов криптографической защиты.

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

3.18. Контролировать и требовать соблюдения установленных правил по организации парольной защиты в ИСПДн.

3.19. Осуществлять оперативный контроль за работой пользователей защищенных АРМ, анализировать содержимое журналов событий операционных систем, систем управления базами данных, пакетов прикладных программ и СЗИ всех АРМ и адекватно реагировать на возникающие нештатные ситуации. 3.20. Обеспечивать своевременное архивирование журналов событий АРМ и надлежащий режим хранения данных архивов

3.21. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания АРМ

и отправке их в ремонт (контролировать стирание информации на съемных носителях).

3.22. Организовывать учет, хранение, прием и выдачу персональных идентификаторов ответственным исполнителям, осуществлять контроль за правильностью их использования.

3.23. Осуществлять периодический контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных.

3.24. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах по управлению СЗИ, установленных на АРМ ИСПДн.

3.25. Требовать от пользователей стирания остаточной информации на несъемных носителях (жестких дисках) установленным порядком, а в оперативной памяти по окончании обработки информации путем перезагрузки АРМ; 3.26. Контролировать обеспечение защиты конфиденциальной информации при взаимодействии абонентов с информационными сетями связи общего пользования

3.27. Проводить работу по выявлению возможности вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам АРМ.

3.28. Докладывать ответственному по обеспечению безопасности о выявленных угрозах безопасности информации, обрабатываемой в ИСПДн, об имевших место попытках НСД к информации и техническим средствам АРМ.

3.29. Проводить занятия с пользователями ИСПДн по правилам работы на АРМ, оснащенных СЗИ, и по изучению руководящих документов по вопросам обеспечения безопасности информации с разбором недостатков, выявленных при контроле эффективности защиты информации.

3.30. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в ИСПДн.

4. ПРАВА

4.1. Требовать от сотрудников ДОУ выполнения установленных правил обработки и защиты персональных данных.

4.2. Требовать от сотрудников ДОУ прекращения обработки персональных данных в случае их неправомерного использования и нарушения установленного порядка обработки.

4.3. Вносить предложения по совершенствованию организационных и технических мер.

4.4. Принимать участие в рассмотрении обращений и запросов субъектов персональных данных

4.5. Требовать от руководства ДОУ организационного и материально-технического обеспечения своей деятельности, а также оказания содействия в исполнении своих обязанностей и прав.

5. ОТВЕТСТВЕННОСТЬ

5.1. За разглашение информации ограниченного доступа, ставшей известной ему по роду работы, в соответствии с законодательством РФ.

5.2. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в пределах, определенных действующим трудовым законодательством РФ.

5.3. За причинение материального ущерба управлению образования в пределах, определенных действующим трудовым и гражданским законодательством РФ.

5.4. За правонарушения, совершенные в процессе осуществления своей деятельности, в пределах определенных действующим административным, уголовным и гражданским законодательством РФ.

Заведующий МБДОУ д/с №8 «Буратино» Каденцева А.Е.