Государственное бюджетное дошкольное образовательное учреждение
детский сад № 8
Пушкинского района Санкт–Петербурга

ПРИКАЗ

от 17.11.2022 **№ 94-ОД**

«О назначении ответственных
за защиту информации»

Во исполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17

ПРИКАЗЫВАЮ:

П.1. Назначить ответственными лицами за организацию обработки персональных данных в ГБДОУ детском саду № 8 Пушкинского района Санкт-Петербурга:
- специалиста по кадрам Кузичеву Е.И.
- специалиста по кадрам Полякову М.В.

П.1.1. Утвердить и ввести в действие инструкцию ответственного за организацию обработки персональных данных согласно приложению № 1.

П.2. Утвердить перечень лиц, имеющих доступ и осуществляющие обработку персональных данных:

П.2.1. Перечень лиц, допущенных к обработке персональных данных работников:
- заведующий Никифорова И.Н.
- заместитель заведующего по учебно-воспитательной работе Бесфамильная Н.Е.
- заместитель заведующего по административно-хозяйственной части Шаньгина Е.А.
- заведующий производством (шеф-повар) (вакансия).
- специалист по кадрам Кузичева Е.И.
- специалист по кадрам Полякова М.В.
- сотрудники СПБ «ГКУ Централизованная бухгалтерия Пушкинского района».

П.2.2. Перечень лиц, допущенных к обработке персональных данных родителей (законных представителей) и воспитанников:
- заведующий Никифорова И.Н.
- заместитель заведующего по учебно-воспитательной работе Бесфамильная Н.Е.
- специалист по кадрам Кузичева Е.И.
- специалист по кадрам Полякова М.В.
- воспитатель Зарудная А.В.
- сотрудники СПБ «ГКУ Централизованная бухгалтерия Пушкинского района».

П.2.3. Перечень должностей, имеющих ограниченный допуск в рамках своих должностных обязанностей к персональным данным родителей (законных представителей) и воспитанников:
- воспитатель;
- учитель-логопед;
- педагог-психолог;
- врач и медицинская сестра.

П.2.4. Утвердить и ввести в действие инструкцию ответственного за обработку персональных данных.

П.2.5. Ответственным лицам в своей работе строго руководствоваться действующим законодательством Российской Федерации в отношении обработки и защиты персональных данных.

П.3. Утвердить номера кабинетов, в границах которых происходит работа с персональными данными:

- кабинет заведующего № 205;
- кабинет специалистов по кадрам № 206.

П.4. Утвердить и ввести в действие следующие инструкции:

- Инструкцию пользования персональным компьютером согласно приложению № 3;
- Инструкцию по работе работников в сети Интернет согласно приложению № 4;
- Инструкцию пользователя в случае возникновения нештатных ситуаций согласно приложению № 5;
- Инструкцию по защите персональных данных согласно приложению № 6;
- Инструкцию пользователям автоматизированных систем по организации антивирусной защиты согласно приложению № 7.

П.5. Утвердить Матрицу доступа к информационным ресурсам автоматизированных систем управления (АИСУ) программно-технологического комплекса «ПараГраф» и информационной системой СБИС согласно приложению № 8.

П.6. В связи с возможной угрозой вирусной атаки запретить работникам использовать USB-флеш-накопители.

П.7. Специалистам по кадрам Кузичевой Е.И., Поляковой М.В. ознакомить с данным приказом и с содержанием инструкций работников под подпись.

П.8. Контроль за выполнением приказа оставляю за собой.

Приложение № 9: «Подписи сотрудников».

Заведующий **И.Н. Никифорова**

Приложение № 1 к приказу от 17.11.2022 № 94-ОД

ИСТРУКЦИЯ
ответственного за организацию обработки персональных данных

Настоящая должностная инструкция разработана и утверждена в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правыми актами, операторами, являющимися государственными или муниципальными органами, Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», локальными актами государственного бюджетного дошкольного образовательного учреждения детского сада № 8 Пушкинского района Санкт-Петербурга.

1. Общие положения

1.1. Ответственный за организацию обработки персональных данных относится к категории специалистов и непосредственно подчиняется заведующему государственного бюджетного дошкольного образовательного учреждения детского сада № 8 Пушкинского района Санкт-Петербурга (далее – ГБДОУ № 8).

1.2. Ответственный за организацию обработки персональных данных является сотрудником ГБДОУ № 8 и назначается приказом заведующего.

1.3. Ответственный за организацию обработки персональных данных обладает правами доступа к любым носителям персональных данных.

1.4. Ответственный за организацию обработки персональных данных должен знать:

- законодательство Российской Федерации в области работы и защиты персональных данных;
- порядок систематизации, учета и ведения документации с использованием современных информационных технологий;
- правила и нормы охраны труда.

2. Должностные обязанности

Ответственный за организацию обработки персональных данных обязан:

2.1. Осуществлять внутренний контроль за соблюдением законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

2.2. Доводить до сведения работников организации положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

2.3. Знать перечень и условия обработки персональных данных.

2.4. Знать и предоставлять на утверждение заведующему изменения к списку лиц, доступ которых к персональным данным необходим для выполнения ими своих служебных (трудовых) обязанностей.

2.5. Осуществлять учёт документов, содержащих персональные данные и организовывать процедуру их уничтожения.

2.6. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

2.7. Реагировать на попытки несанкционированного доступа к информации, содержащей персональные данные.

2.8. Контролировать осуществление мероприятий по установке и настройке средств защиты информации.

2.9. Проводить занятия и инструктажи с сотрудниками ГБДОУ № 8 о порядке работы с

персональными данными и изучение руководящих документов в области обеспечения безопасности персональных данных.

2.10. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

2.11. Представлять интересы ГБДОУ № 8 при проверках надзорных органов в сфере обработки персональных данных.

2.12. Знать законодательство РФ о персональных данных, следить за его изменениями.

2.13. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

3. Права

Ответственный за организацию обработки персональных данных имеет право:

3.1. Требовать от сотрудников выполнения локальных нормативно-правовых актов в части работы с персональными данными.

3.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.3. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

4. Ответственность

4.1. Ответственный за организацию обработки персональных данных несёт персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия.

4.2. Ответственный за организацию обработки персональных данных при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 2 к приказу от 17.11.2022 № 94-ОД

Инструкция
ответственного за обработку персональных данных

1. Общие положения

1.1. Настоящая инструкция определяет обязанности, права и ответственность ответственного за обработку персональных данных.
1.2. Ответственный за обработку персональных данных в своей деятельности руководствуется:
- действующими нормативными документами по вопросам выполняемой работы;
- уставом образовательной организации и локальными нормативными актами;
- настоящей инструкцией.

1.4. Ответственный за обработку персональных данных должен знать:
- трудовое законодательство;
- документы, определяющие политику Оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- методы применения правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- меры осуществления внутреннего контроля и (или) аудита соответствия обработки персональных данных;
- порядок оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим федеральным законом;
- алгоритм ознакомления работников Оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;
- порядок разработки нормативных материалов для защиты персональных данных.

2. Должностные обязанности

Ответственный за обработку персональных данных обязан:
2.1. Организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.
2.2. Организовывать и осуществлять внутренний контроль за соблюдением уполномоченными на обработку персональных данных требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных.
2.3. Организовывать доведение до сведения уполномоченных на обработку персональных данных положений законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.
2.4. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов.
2.5. В случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

2.6. Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.
2.7. Доводить до сведения работников Оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.
2.8. Блокировать неправомерно обрабатываемые персональные данные, прекращать обработку персональных данных в соответствии с законодательством Российской Федерации.
2.9. Уведомлять субъектов персональных данных об устранении допущенных нарушений при обработке их персональных данных.
2.10. Проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации о персональных данных, соотношения указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации в области обработки и защиты персональных данных.
2.11. Участвовать в рассмотрении проектов решений по вопросам своей компетенции.

3. Права

Ответственный за обработку персональных данных имеет право:
3.1. Знакомиться с проектами решений заведующего, касающимися его деятельности.
3.2. Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с обязанностями, предусмотренными настоящей инструкцией.
3.3. Получать информацию и документы, необходимые для выполнения своих должностных обязанностей.
3.4. Требовать от заведующего оказания содействия в исполнении своих должностных обязанностей и прав.

4. Ответственность

Ответственный за обработку персональных данных несет ответственность:
4.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.
4.2. За нарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.
4.3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

5. Порядок пересмотра инструкции

5.1. Данная инструкция пересматривается, изменяется и дополняется по мере необходимости.
5.2. С приказом о внесении изменений (дополнений) в инструкцию знакомятся под подпись все работники организации, на которых распространяется действие этой инструкции.

Приложение № 3 к приказу от 17.11.2022 № 94-ОД

Инструкция
пользования персональным компьютером

Персональные компьютеры, серверы, программное обеспечение, вся информация, хранящаяся на них и вновь создаваемая, оборудование локальной вычислительной сети, коммуникационное оборудование являются собственностью Государственного бюджетного дошкольного образовательного учреждения детский сад № 8 Пушкинского района Санкт-Петербурга (далее ГБДОУ). предоставляются работникам для осуществления ими их должностных обязанностей.

1. Общие положения

1.1. Целью настоящей инструкции является регулирование работы пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации. Более эффективного использования сетевых ресурсов и уменьшить риск умышленного или неумышленного неправильного их использования;
1.3. Работа в системе каждому работнику разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо согласовать это с руководством;
1.7. Каждый сотрудник сам создает пароль для входа в ПК;
1.8. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в компьютер, передача их кому-либо запрещена;
1.9. В случае нарушения правил пользования ПК, связанных с используемым им компьютером, пользователь сообщает руководству, которое проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений;
1.10. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере ли каком-либо другом, пользователь должен немедленно сообщить об этом руководству;
1.14. Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления пользователя с инструкцией лежит на руководителе.

2. Работа за компьютером

2.1. Запрещено самостоятельно разбирать компьютер и все его комплектующие.
2.2. Все кабели, соединяющие системный блок с другими устройствами, следует вставлять и вынимать только при выключенном компьютере.
2.3. Запрещено самостоятельно устанавливать, удалять, деактивировать и изменять программное обеспечение и сетевые настройки на компьютере.
2.4. Запрещено аварийно завершать работу компьютера кнопкой "Reset" или отключением от электросети. Завершайте работу компьютера правильно, через кнопку (Пуск);
2.5. Запрещено подвергать компьютер и периферийные устройства физическим, термическим и химическим воздействиям. (Нельзя сидеть на компьютере, проливать на него чай, кофе, просыпать семечки, ставить у батареи и других нагревательных приборов);
2.5. По завершению рабочего дня компьютер необходимо выключить, и обесточить;
2.6. Перед началом работы пользователь должен:
* Включить выключатель сетевого фильтра. При включении кнопка должна начать светиться;
* Включить источник бесперебойного питания (ИБП) и выждать 5 секунд;
* Включить монитор (если выключен);
* Включить компьютер кнопкой "Power". Дождаться загрузки операционной системы (ОС);
* Войти в систему, используя свои личные имя пользователя и пароль.
2.7. По завершению работы пользователь должен:
* Закрыть все открытые программы и документы, сохранив нужные изменения;
* С помощью меню "Пуск->Завершение работы" выключить компьютер и дождаться завершения работы. (Системный блок перестанет мигать и шуметь);
* Выключить монитор;
* Выключить источник бесперебойного питания (ИБП), нажав кнопку на передней панели;
* Выключить сетевой фильтр.

2.8. При отключении электроэнергии источник бесперебойного питания (ИБП) позволяет компьютеру оставаться в рабочем состоянии от 5 до 20 минут. При отключении электроэнергии в помещении пользователь должен в немедленном порядке провести правильное выключение компьютера.

3. Работа с электронной почтой

3.1. Электронная почта предоставляется сотрудникам организации только для выполнения своих прямых служебных обязанностей. Использование ее в личных целях запрещено.
3.2. Все электронные письма, создаваемые и хранимые на компьютерах организации, являются собственностью организации и не считаются персональными;
3.3. Организация оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины. Содержимое электронного письма не может быть раскрыто, кроме как с целью обеспечения безопасности или по требованию правоохранительных органов;
3.4. Конфигурировать программы электронной почты так, чтобы стандартные действия пользователя, использующие установки по умолчанию, были бы наиболее безопасными;
3.5. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение политики безопасности фирмы;
3.6. Пользователи не должны позволять кому-либо посылать письма от чужого имени.
3.7. Организация оставляет за собой право осуществлять наблюдение за почтовыми отправлениями сотрудников. Электронные письма могут быть прочитаны организацией, даже если они были удалены и отправителем, и получателем. Такие сообщения могут использоваться для обоснования наказания;
3.8. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы;
3.9. Осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается, как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

4. Работа в сети Интернет

4.2. Пользователи используют программы для поиска информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей;
4.3. По использованию Интернет ведется статистика и поступает в архив фирмы. В конце каждого месяца все пользователи сети Интернет заполняет и подписывает личную статистку по использованию ресурсов сети;
4.4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций;
4.5. Сотрудникам организации, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство РФ;
4.8. Запрещено получать и передавать через сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую тайну, распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения;
4.9. Запрещено получать доступ к информационным ресурсам сети или сети Интернет, не являющихся публичными, без разрешения их собственника.

Приложение № 4 к приказу от 17.11.2022 № 94-ОД

ИНСТРУКЦИЯ
по работе работников в сети Интернет

Общие положения

Настоящая инструкция устанавливает порядок действий работников при работе с ресурсами и сервисами сети Интернет.

Ознакомление с инструкцией и ее соблюдение обязательны для работников ГБДОУ детского сада № 8, а также иных лиц, допускаемых к работе с ресурсами и сервисами сети Интернет.

Настоящая инструкция имеет статус локального нормативного акта. Если нормами действующего законодательства Российской Федерации предусмотрены иные требования, чем настоящей инструкцией, применяются нормы действующего законодательства.

Организация использования сети Интернет

Доступ к ресурсам, несовместимым с целями и задачами образования и воспитания, запрещен.

При использовании сети Интернет в ГБДОУ детском саду № 8 предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к образовательному процессу.

При использовании ресурсов сети Интернет обязательным является соблюдение законодательства об интеллектуальных правах и иного применимого законодательства.

Работники ГБДОУ детского сада № 8, имеющие рабочее место, оборудованное компьютером с подключением к сети Интернет, использует сеть в любое время в рамках режима работы учреждения.

При использовании сетевых сервисов, предполагающих авторизацию, запрещается пользоваться чужими учетными данными.

Все компьютеры, подключаемые к сети Интернет, обязаны иметь установленное, действующее и обновляющееся антивирусное программное обеспечение.

Права, обязанности и ответственность пользователей

Использование ресурсов сети Интернет в ГБДОУ детском саду № 8 осуществляется в целях организации трудовых отношений и образовательного процесса.

К работе в сети Интернет допускаются лица, прошедшие инструктаж и обязавшиеся соблюдать правила работы.

Пользователям запрещается:

- посещать сайты, содержание и тематика которых недопустимы для несовершеннолетних и (или) нарушают законодательство Российской Федерации (порнография, эротика, пропаганда насилия, терроризма, политического и религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);
- загружать и распространять материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения,
- уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, а также размещение ссылок на выше указанную информацию;
-загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
-распространять информацию, порочащую честь и достоинство граждан;
-осуществлять любые сделки через сеть Интернет;
-работать с объемными ресурсами (видео, аудио, чат, фото) без согласования;

Пользователи несут ответственность:

- за содержание передаваемой, принимаемой и печатаемой информации;

- за нанесение любого ущерба оборудованию (порча имущества, вывод оборудования из рабочего состояния)
- пользователь несет материальную ответственность в соответствии с законодательством.

Действия в нештатных ситуациях:

- При утрате (в том числе частично) подключения к сети Интернет лицо, обнаружившее неисправность, сообщает об этом ответственному работнику за организацию подключения к сети Интернет;
- При заражении компьютера вирусами его использование немедленно прекращается работником, обнаружившим заражение. О сложившейся ситуации сообщается ответственному лицу за организацию подключения к сети Интернет. Компьютер отключается от сети до момента очистки от всех вирусов. Разрешение на; дальнейшее использование компьютера и подключение его к сети дает лицо, ответственное за организацию подключения к сети Интернет после соответствующей проверки.

Приложение № 5 к приказу от 17.11.2022 № 94-ОД

ИНСТРУКЦИЯ
пользователю в случае возникновения
нештатных ситуаций

1. Общие положения

1.1. Настоящая Инструкция определяет действия работников ГБДОУ № 8 по применению основных мер, методов и средств сохранения (поддержания) работоспособности автоматизированной системы (далее - АС) при возникновении различных кризисных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности АС и ее основных компонентов. Кроме того, она описывает действия различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

1.2. Под *кризисной ситуацией* понимается ситуация, возникшая в результате нежелательного воздействия на АС, не предотвращенная средствами защиты. Кризисная ситуация может возникнуть в результате злого умысла или случайно (в результате непреднамеренных действий, пожаров, аварий, стихийных бедствий и т.п.).

Под *умышленным нападением* понимается кризисная ситуация, которая возникла в результате выполнения злоумышленниками в определенные моменты времени заранее обдуманных и спланированных действий.

Под *случайной (непреднамеренной) кризисной ситуацией* понимается такая кризисная ситуация, которая не была результатом заранее обдуманных действий и возникновение которой, явился результат объективных причин случайного характера, халатности, небрежности или случайного стечения обстоятельств.

По степени серьезности и размерам наносимого ущерба, кризисные ситуации разделяются на следующие категории:

Угрожающая - приводящая к полному выходу АС из строя и ее неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации;

Серьезная - приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа.

Ситуации, возникающие в результате нежелательных воздействий, не наносящих ощутимого ущерба, но, тем не менее, требующие внимания и адекватной реакции (например, зафиксированные неудачные попытки проникновения или несанкционированного доступа к ресурсам системы) к критическим не относятся. Действия в случае возникновения таких ситуаций предусмотрены Планом защиты.

1.3. Источники информации о возникновении кризисной ситуации:

- пользователи, обнаружившие несоответствия или иные подозрительные изменения в работе или конфигурации системы или средств ее защиты в своей зоне ответственности;
- средства защиты или сигнализации, обнаружившие кризисную ситуацию;
- системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

2. Меры обеспечения непрерывной работы и восстановления автоматизированной системы

2.1. Непрерывность процесса функционирования АС и своевременность восстановления ее работоспособности достигается:

- проведением специальных организационных мероприятий и разработкой организационно-распорядительных документов по вопросам обеспечения непрерывности вычислительного процесса;
- строгой регламентацией процесса обработки информации с применением АРМ и действий персонала системы, в том числе в кризисных ситуациях;

- назначением и подготовкой должностных лиц, отвечающих за организацию и осуществление практических мероприятий по обеспечению непрерывности вычислительного процесса;
- четким знанием и строгим соблюдением всеми должностными лицами, использующими средства вычислительной техники АС, требований руководящих документов по обеспечению непрерывности вычислительного процесса;
- применением различных способов резервирования аппаратных ресурсов, эталонного копирования программных и страхового копирования информационных ресурсов системы;
- эффективным контролем за соблюдением требований по обеспечению непрерывности вычислительного процесса должностными лицами и ответственным;
- постоянным поддержанием необходимого уровня защищенности компонентов системы, непрерывным управлением и административной поддержкой корректного применения средств защиты;
- проведением постоянного анализа эффективности принятых мер и применяемых способов и средств обеспечения непрерывности вычислительного процесса, разработкой и реализацией предложений по их совершенствованию.

3. Общие требования

Все пользователи, работа которых может быть нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, должны немедленно оповещаться. Дальнейшие действия по устранению причин нарушения работоспособности АС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

Каждая кризисная ситуация должна анализироваться, и по результатам этого анализа должны вырабатываться предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т.п.

Серьезная и угрожающая кризисная ситуация могут требовать оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи в серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранением копий.

Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность системы и выполнение ею своих задач (системное и прикладное программное обеспечение, базы данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

Все программные средства, используемые в системе должны иметь эталонные (дистрибутивные) копии. Их местонахождение и сведения об ответственных за их создание,хранение и использование должны быть указаны в формулярах на каждую ПЭВМ (рабочую станцию). Там же должны быть указаны перечни наборов данных, подлежащих страховому копированию, периодичность копирования, место хранения и ответственные за создание, хранение и использование страховых копий данных.

Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных должны быть отражены в функциональных обязанностях соответствующих категорий персонала.

Каждый носитель, содержащий резервную копию, должен иметь метку, содержащую данные о классе, ценности, назначении хранимой информации, ответственном за создание, хранение и использование, дату последнего копирования, место хранения и др.

Дублирующие аппаратные ресурсы предназначены для обеспечения работоспособности системы в случае выхода из строя всех или отдельных аппаратных компонентов в результате угрожающей кризисной ситуации. Количество и характеристики дублирующих ресурсов должны обеспечивать выполнение основных задач системой в любой из предусмотренных кризисных ситуациях.

Ликвидация последствий угрожающей или серьезной кризисной ситуации подразумевает, возможно, более полное восстановление программных, аппаратных, информационных и других поврежденных компонентов системы. Для восстановления используются средства, перечисленные ниже.

В случае возникновения любой кризисной ситуации должно производиться расследование причин ее возникновения, оценка причиненного ущерба, определение виновных и принятие соответствующих мер.

Расследование кризисной ситуации производится группой, назначаемой руководством учреждения. Выводы группы докладываются непосредственно руководству учреждения.

Если причиной угрожающей или серьезной кризисной ситуации явились недостаточно жесткие меры защиты и контроля, а ущерб превысил установленный уровень, то такая ситуация является основанием для полного пересмотра планов обеспечения непрерывной работы и восстановления.

Кризисные ситуации, предусмотренные планом обеспечения непрерывной работы и восстановления

1. К *угрожающим кризисным ситуациям* относятся:

* нарушение подачи электроэнергии в здании;
* выход из строя файлового сервера (с потерей информации);
* выход из строя файлового сервера (без потери информации);
* частичная потеря информации на сервере без потери его работоспособности;
* выход из строя локальной сети (физической среды передачи данных);

2. К *серьезным кризисным ситуациям* относятся:

* выход из строя рабочей станции (с потерей информации);
* выход из строя рабочей станции (без потери информации);
* частичная потеря информации на рабочей станции без потери ее работоспособности;

3. К *ситуациям, требующим внимания* относятся:

* несанкционированные действия, заблокированные средствами защиты и зафиксированные средствами регистрации.

Приложение № 6 к приказу от 17.11.2022 № 94-ОД

ИНСТРУКЦИЯ
по защите персональных данных

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.

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.

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 образовательной организации.

1. «Внутренняя защита»

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами образовательной организации. Для 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 работниками 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 другими работниками;
- воспитательная и разъяснительная работа с работниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- персональные компьютеры, на которых содержатся персональные данные, должны быть защищены паролями доступа и антивирусной защитой.

2. «Внешняя защита»

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. Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности образовательной организации, посетители. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

Для защиты персональных данных работников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим образовательной организации;
- порядок охраны территории, здания, помещения, транспортных средств;
- требования к защите информации при интервьюировании и собеседованиях.

Приложение № 7 к приказу от 17.11.2022 № 94-ОД

Инструкция
пользователям автоматизированных систем
по организации антивирусной защиты

1. Общие положения

Настоящая Инструкция определяет требования к организации защиты автоматизированных систем (АС) Государственного бюджетного дошкольного образовательного учреждения детский сад № 8 Пушкинского района Санкт-Петербурга (далее ГБДОУ) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих и сопровождающих АС Предприятия, за их выполнение.

К использованию в ГБДОУ допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и рекомендованные к применению специалистами отдела защиты информации.

Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на рабочих станциях (ПЭВМ), серверах ЛВС Предприятия осуществляется специалистами отдела главного инженера в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

Ежедневно в начале работы при загрузке средств вычислительной техники (ПЭВМ) (для серверов ЛВС - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенной автономной ПЭВМ, или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты, - на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться **не реже одного раза в месяц**.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе со специалистом отдела главного инженера или системного администратора должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники Организации обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения, специалистов отдела защиты информации, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести «лечение» или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь специалистов отдела защиты информации);
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми

антивирусными средствами, направить зараженный вирусом файл в специальную карантинную зону, на специально выделенном для этого каталоге (при необходимости для выполнения требований данного пункта привлечь специалистов отдела защиты информации);

- все факты обнаружения зараженных вирусом файлов записываются в служебный журнал, где отображается тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

Ответственность за организацию антивирусного контроля в ГБДОУ, возлагается на заместителя заведующего по учебно-воспитательной работе, заместителя по административно-хозяйственной части.

Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на руководителя и всех сотрудников, являющихся пользователями автоматизированных систем.

Периодический контроль за состоянием антивирусной защиты в автоматизированной системе ГБДОУ, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками ГБДОУ осуществляется руководителем.

Приложение № 8 к приказу от 17.11.2022 № 94-ОД

МАТРИЦА ДОСТУПА
к информационным ресурсам автоматизированных систем управления (АИСУ) программно-технологического комплекса «ПараГраф»

№ п/п	Фамилия, Имя, Отчество	Должность	Право доступа к персональным данным			
			Чтение	Запись	Изменение	Удаление
1.	Никифорова Ирина Николаевна	Заведующий ГБДОУ № 8	+	-	-	-
2.	Бесфамильная Наталья Евгеньевна	Заместитель заведующего по УВР	+	-	-	-
3.	Зарудная Анжела Валерьевна	Воспитатель	+	+	+	+
4.	Кузичева Екатерина Ивановна	Специалист по кадрам	+	+	+	+
5.	Полякова Марина Владимировна	Специалист по кадрам	+	+	+	+

МАТРИЦА ДОСТУПА
к информационной системе СБИС

№ п/п	Фамилия, Имя, Отчество	Должность	Право доступа к персональным данным			
			Чтение	Запись	Изменение	Удаление
1.	Никифорова Ирина Николаевна	Заведующий ГБДОУ № 8	+	-	-	-
2.	Кузичева Екатерина Ивановна	Специалист по кадрам	+	+	+	+
3.	Полякова Марина Владимировна	Специалист по кадрам	+	+	+	+