Муниципальное бюджетное дошкольное образовательное учреждение
Центр развития ребенка – детский сад № 13

Приказ

от 09.01. 2020 г. № 9

"Об утверждении порядка обработки и защиты персональных данных и возложении обязанностей на должностных лиц МБДОУ ЦРР- детский сад № 13"

I.В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»» и Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" (Собрание законодательства Российской Федерации, 2007, N 48, часть II, ст. 6001) приказываю:

1.Ввести режим обработки персональных данных.

2.Создать комиссию по защите персональных данных в МБДОУ ЦРР-детский сад № 13 в следующем составе:
Председатель – Е.И. Архиреева (заведующая МБДОУ № 13)
члены комиссии – Н.В. Рышкова (делопроизводитель),
– Т.В. Пожигаева (зам.зав. по АХЧ).

II. Для выполнения требований нормативных документов в сфере обработки персональных данных:

Возложить обязанности ответственного за организацию обработки персональных данных в МБДОУ № 13 на Рышкову Н.В.

1.Определить следующие обязанности ответственному за организацию обработки персональных данных МБДОУ № 13:

-осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

-доводить до сведения работников положения законодательства Российской Федерации о персональных данных, Федеральных и Региональных нормативных документов по вопросам обработки персональных данных, требований к защите персональных данных;

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

1. Возложить обязанности администратора по защите информации (безопасности ИСПДн) МБДОУ № 13 на Рышкову Н.В.

2. Определить функциональные обязанности (Приложение № 1) к данному приказу администратору безопасности информации в автоматизированных системах объектов информатизации МБДОУ № 13.

3. Ознакомить Рышкову Н.В. с функциональными обязанностями под роспись.

4. Заведующему Архиреевой Е.И. ознакомить сотрудников МБДОУ № 13 с «Инструкцией администратору ИСПДн МБДОУ № 13 «Инструкцией по проведению антивирусного контроля ИСПДн МБДОУ № 13 и «Инструкцией пользователям ИСПДн МБДОУ детский сад №13 под роспись.

III.Назначить ответственных за обработку персональных данных в информационных системах персональных данных:

- старший воспитатель Бойко Л.Ф. (данные воспитанников и их родителей (законных представителей) и сотрудников);

-старшая медсестра Иванова О.С. (данные воспитанников и их родителей (законных представителей) и сотрудников);

-воспитатели групп (данные воспитанников и их родителей (законных представителей) своих групп);

-заместитель заведующей по АХЧ Пожигаева Т.В. (данные сотрудников);

-делопроизводитель Рышкова Н.В. (данные воспитанников и их родителей (законных представителей) и сотрудников)

- педагоги – психологи Власенко Г.Г., Григорьева Н.А. (данные воспитанников и их родителей (законных представителей) и сотрудников).

1. Осуществлять доступ лиц, ответственных за обработку персональных данных, на основании Положения о разграничении прав доступа к обрабатываемым персональным данным.

2. Утвердить инструкции пользователей, осуществляющих обработку персональных данных в информационных системах персональных данных.

3.Осуществлять регистрацию обращений субъектов персональных данных в Журнале учета обращений субъектов персональных данных о выполнении их законных прав.

V.1.Разместить настоящий приказ на официальном сайте учреждения в течение десяти рабочих дней со дня издания приказа.

2.Контроль за исполнением настоящего приказа оставляю за собой.

Заведующий МБДОУ _____ Е.И. Архиреева

Приложение 1 к приказу № 9
от 09.01.2020 года

Функциональные обязанности администратора безопасности информации в автоматизированных системах объектов информатизации

Допуск администратора безопасности информации (далее – администратор) для работы в автоматизированных системах объектов информатизации (далее – АС ОИ) осуществляется в соответствии с приказом руководителя МБДОУ № 13 и разрешительной системой доступа.

Администратор имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам компьютера. При этом для хранения файлов, содержащих конфиденциальную информацию, разрешается использовать только специально выделенные каталоги на несъемных носителях информации, а также соответствующим образом учтенные съёмные носители информации.

Присвоение администратору полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы администратора в АС ОИ осуществляется при первичной регистрации администратора ответственным за обеспечение режима ограничения доступа к информации (далее – ответственный за безопасность информации).

Администратор отвечает за правильность включения и выключения технических средств и систем, входа в систему и все действия при работе в АС ОИ

Вход администратора в систему осуществляется на основе ввода имени, присвоенного при первичной регистрации и ввода личного пароля. Требования к парольной защите определяется инструкцией по парольной защите.

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам администратора осуществляется периодическая (раз в месяц) замена пароля постоянного администратора. Замена личного пароля осуществляется администратором самостоятельно.

При работе со съемными носителями информации пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием установленных антивирусных программ, в соответствии с Инструкцией по антивирусной защите.

Администратор обязан:

- знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению принятого режима информационной безопасности;
- обеспечить правильность вводимых данных;

- своевременно сообщать ответственному за безопасность информации об изменениях статуса администратора;
- незамедлительно сообщить ответственному за безопасность информации факты выявления инцидентов с доступом к конфиденциальной информации.
- В процессе работы администратору запрещается:
- использовать для постоянного хранения и обработки конфиденциальной информации каталоги несъемных носителей информации, за исключением выделенных каталогов;
- осуществлять попытки несанкционированного доступа к ресурсам операционной системы;
- в рамках выделенных ресурсов и полномочий доступа к ним обрабатывать информацию с уровнем конфиденциальности, выше заявленного при регистрации;
- пытаться подменять функции ответственного за безопасность информации по перераспределению времени работы и полномочий доступа к ресурсам компьютера;
- покидать помещение с незаблокированной учетной записью;
- отключать установленные средства защиты информации;
- использовать машинные носители без их предварительной проверки антивирусными средствами;
- устанавливать программное обеспечение;
- менять параметры конфигурации ранее установленных программных средств;
- использовать пароль, предоставленный ответственным за безопасность информации для первоначального доступа в качестве постоянного рабочего пароля;
- использование различными администраторами одной и той же учетной записи, даже если администраторы имеют одинаковые полномочия по доступу;
- запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа другим лицам, в том числе и своим руководителям;
- хранение пароля на любых твердых носителях, позволяющих другим лицам получить информацию о пароле;
- использовать информацию, полученную в результате доступа к БД, в целях, не предусмотренных его функциональными обязанностями.

Ответственность за сохранность и правильное использование информации, ставшей известной в процессе обработки конфиденциальной информации несет администратор.

Возможность получения технического доступа к конфиденциальной информации не дает права администратору обработки такой информации если им не предоставлены права доступа к этой информации. Такие действия рассматриваются как попытки несанкционированного доступа.

При выявлении инцидентов с доступом к конфиденциальной информации доступ администратора к ней может быть ограничен до окончания расследования инцидента, о чем администратор уведомляется в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к конфиденциальной информации, материалы расследования могут быть направлены в соответствующие службы для привлечения нарушителя к ответственности.

Администратор несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования этой учетной записи.

При нарушениях администратором правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.