Утверждена
Приказом от
«09» 01 2019г. №41-од
Заведующий
_____С.Г.Кузина
(приложение №1)

Инструкция
администратора безопасности информационных систем
персональных данных МБДОУ «Детский сад №229» г.о. Самара

1. Общие положения

1.1. Настоящая инструкция определяет основные права и обязанности администратора безопасности информационных система персональных данных муниципального бюджетного дошкольного образовательного учреждения «Детский сад №229» городского округа Самара (далее–МБДОУ).

1.2. Администратор безопасности информационных систем персональных данных (далее –ИСПДн) является работником МБДОУ и назначается приказом заведующего МБДОУ.

1.3. Администратор безопасности ИСПДн обладает правом доступа к любым программным и аппаратным ресурсам МБДОУ.

2. Термины и определения

2.1. В настоящей инструкции используются следующие термины и определения:

персональные данные – любая информация, относящаяся к физическому лицу (субъекту персональных данных),

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;

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

информационная система персональных данных (ИСПДн) – совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием или без использования средств автоматизации;

информация – любые сведения (сообщения, данные) независимо от формы их представления;

автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства (принтер, многофункциональные устройства, сканеры и т.д.);

доступ к информации – возможность получения информации и ее использования;

защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности;

несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей, в компьютерных базах данных, файловых хранилищах, архивах и т.д. путем изменения (повышения, фальсификации) своих прав доступа;

носитель информации – любой материальный объект или среда, используемые для хранения или передачи информации;

средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации;

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 становится невозможным восстановить содержание персональных данных в ИСПДн и (или) в результате которых уничтожаются материальные носители персональных данных.

3. Обязанности администратора

3.1. Администратор безопасности ИСПДн обязан:

знать перечень и условия обработки персональных данных в МБДОУ;

знать перечень установленных в кабинетах МБДОУ технических средств, в том числе съемных носителей, конфигурацию ИСПДн и перечень задач, решаемых с ее использованием;

определять полномочия пользователей ИСПДн (оформление разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей;

осуществлять учет и периодический контроль над составом и полномочиями

пользователей автоматизированных рабочих мест (АРМ);

блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки;

реагировать на попытки несанкционированного доступа к информации в установленном п.4 настоящей Инструкции порядке;

осуществлять непосредственное управление и контроль режимов работы применяемых в ИСПДн средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование);

проводить работу по выявлению возможных каналов утечки персональных данных, изучать текущие тенденции в области защиты персональных данных;

проводить разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации;

вносить плановые и внеплановые изменения в учетную запись пользователей ИСПДн, в том числе в связи с увольнением работника;

осуществлять периодическое резервное копирование баз персональных данных и сопутствующей информации, а также внеплановое, если это необходимо для обеспечения сохранности персональных данных;

осуществлять восстановление информации из резервных копий по требованию пользователей ИСПДн;

хранить дистрибутивы программного обеспечения, установленного в ИСПДн, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц;

вносить предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятию мер по предотвращению возможных опасных последствий нарушений;

знать законодательство о персональных данных, следить за его изменениями;

выполнять иные мероприятия, требуемые техническими и программными средствами ИСПДн для поддержания их функционирования.

4. Действия при обнаружении попыток несанкционированного доступа

4.1.К попыткам несанкционированного доступа относятся:

сеансы работы с ИСПДн незарегистрированных пользователей, или пользователей,

нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

действия третьего лица, пытающегося получить доступ к ИСПДн (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн или любым другим методом.

4.2. При выявлении факта несанкционированного доступа администратор безопасности ИСПДн обязан:

прекратить несанкционированный доступ к ИСПДн;

доложить заведующему МБДОУ о факте несанкционированного доступа, его результатах (успешный, неуспешный) и предпринятых действиях.

5. Права

5.1. Администратор безопасности ИСПДн имеет право:

требовать от пользователей ИСПДн выполнения инструкций в части работы с программными, аппаратными средствами ИСПДн и персональными данными;

блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных;

проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ;

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

6. Ответственность

6.1. Администратор безопасности ИСПДн несет персональную ответственность за соблюдение требований настоящей инструкции; за средства защиты информации, применяемые в МБДОУ, за качество проводимой им работы по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. Администратор безопасности ИСПДн при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную и иную ответственность в соответствии с законодательством Российской Федерации.

Ознакомлены: _____/ Ханочева О.С.