Утверждаю:
Заведующий МАДОУ д/с № 7

Е.В. Дрижика

Приказ № 68 от 20.07.2021 г.

Инструкция

ответственного за организацию обработки и защиты персональных данных в МАДОУ д/с № 7

1. Общие положения

1. Настоящая инструкция за организацию обработки и защиты персональных данных (далее – Инструкция) определяет функциональные обязанности, права и ответственность ответственного за организацию обработки персональных данных в Муниципальном автономном дошкольном образовательном учреждении детском саду комбинированного вида № 7 (далее – ДОУ), в котором обрабатываются персональные данные (далее – ПДн).

2. Настоящая инструкция подготовлена в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

3. В Инструкции используются следующие понятия и определения:

1) автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

2) база данных- объективная форма представления и организации совокупности данных, систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью электронно-вычислительных машин (ЭВМ)

3) информация- сведения, сообщения, данные) независимо от форма их представления

4) персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)

5) информационная система персональных данных –совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

6) компрометация пароля - утрата доверия к тому, что используемый пароль обеспечивает безопасность персональных данных. К событиям, приводящим к компрометации пароля, относятся следующие события (включая, но не ограничиваясь):

- несанкционированное сообщение пароля другому лицу;

- утеря бумажного или машинного носителя информации, на котором был записан пароль;

- запись пароля на бумажном, машинном, ином носителе информации, доступ к которому не контролируется;

7) конфиденциальность персональных данных - обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

8) несанкционированный доступ к персональным данным - доступ к персональным данным с нарушением установленных прав доступа, приводящий к нарушению конфиденциальности персональных данных, к утечке, искажению, подделке, уничтожению, блокированию доступа к персональным данным;

9) 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;

10) распространение персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

11) разглашение персональных данных - распространение персональных данных без согласия субъекта персональных данных или наличия иного законного основания;

12) средство защиты информации (СЗИ) - программные, программно-аппаратные, аппаратные средства, предназначенные и используемые для защиты персональных данных в ИСПДн;

13) утеря пароля - события, приводящие к невозможности восстановления пароля в памяти лица, владеющего данным паролем;

14) электронная вычислительная машина ИСПДн (ЭВМ) - персональный компьютер, предназначенный для автоматизации деятельности пользователей и входящий в состав ИСПДн. В состав ЭВМ входят: системный блок, монитор, клавиатура, мышь, внешние устройства (локальный принтер, сканер и т.д.), программное обеспечение.

II. Обязанности ответственного

4. Ответственный обязан:

1) хранить в тайне персональные данные, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки персональных данных

немедленно информировать ответственного за организацию обработки персональных данных, Администратора ИСПДн;

2) знать и выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах в соответствии с Инструкциями, требованиями, регламентирующими функционирование установленных средств защиты;

3) хранить в тайне свой пароль доступа в ИСПДн ДОУ;

4) использовать для работы только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски и т.д.);

5) в случае необходимости сообщать о необходимости обновления антивирусных баз Администратору ИБ ИСПДн:

6) немедленно ставить в известность Администратора ИСПДн и/или Администратора ИБ ИСПДн:

- в случае утери носителя с конфиденциальной информацией (персональными данными) и/или при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа к ИСПДн ДОУ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

7) в случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в ИСПДн ДОУ технических средств защиты ставить в известность Администратора ИСПДн и/или Администратора ИБ ИСПДн.

5. В случае увольнения ответственный ИСПДн обязан передать вышестоящему руководству все документы и материалы, относящиеся к ИСПДн ДОУ. В том числе: отчеты, инструкции, служебную переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к ИСПДн ДОУ, полученные в течение срока работы.

6. Уборка помещений должна производиться под контролем ответственного ИСПДн, имеющего доступ в помещение и постоянно в нем работающего.

7. Вынос технических средств ИСПДн ДОУ, на которой проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с Администратором ИСПДн или ответственным за организацию обработку персональных данных запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы. В случае действия гарантийных обязательств

фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

8. АРМ, используемые для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора.

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

10. Оперативно докладывать Администратору ИСПДн и Администратору ИБ ИСПДн о случаях возникновения внештатных ситуаций и аварийных ситуаций.

11. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИСПДн. Предпринимаемые меры по возможности согласовать с вышестоящим руководством.

12. Ответственному категорически запрещается:

- передавать, кому бы то ни было, устно или письменно, персональные данные;
- использовать персональные данные при подготовке открытых публикаций, докладов, научных работ и т.д.;
- выполнять работы с документами, содержащими персональные данные, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения Ответственного за организацию обработки персональных данных;
- оставлять на рабочих столах, в столах и незакрытых сейфах документы, содержащие персональные данные, а также оставлять незапертыми и не опечатанными после окончания работы сейфы, помещения и хранилища с документами, содержащими персональные данные;
- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить персональные данные на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенной без присмотра свое АРМ, не активизировав средства защиты информации от НСД (временную блокировку экрана и клавиатуры);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок следует ставить в известность Администратора ИСПДн или Администратора ИБ ИСПДн.

III. Права ответственного

13. Ответственный имеет право:

1) требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей;

2) получать доступ к информации, материалам, техническим средствам, помещениям, необходимых для надлежащего исполнения своих обязанностей.

IV. Ответственность

14. Ответственный несет ответственность за соблюдение требований настоящей инструкции, а также нормативных документов в области защиты информации. За разглашение персональных данных, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.

15. За разглашение персональных данных, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.