Акт
оценки возможного вреда субъектам, чьи персональные данные обрабатываются в информационных системах Муниципального автономного дошкольного образовательного учреждения детский сад № 14 «Орешек»

Комиссия в составе:

Председатель

Члены комиссии

с целью
самостоятельной экспертной оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Муниципальным автономным дошкольным образовательным учреждением детский сад № 14 «Орешек» (далее –МАДОУ) обязанностей, предусмотренных Федеральным законом № 152-ФЗ от 27 июля 2006 г. «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами,

рассмотрев
результаты по сбору и анализу исходных данных на информационные системы персональных данных,

во исполнение требований
пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», о том, что оператор персональных данных самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом о ПДн, и, в частности, к таким мерам относится оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Обществом законодательства в сфере персональных данных,

с учетом разработанных МАДОУ правил оценки вреда, который может быть причинен субъектам персональных данных, ОПРЕДЕЛИЛА:

ТИПЫ актуальных угроз безопасности ПДн	**ОЦЕНКИ возможного вреда субъекту ПДн, определенные членами комиссии**					**Определение возможного вреда (Y2)**
	Эксперт 1	Эксперт 2	Эксперт 3	Эксперт 4	Эксперт 5	
Кража ПЭВМ	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Y2 = 1,0 вред субъектам ПДн высокий
Кража носителей информации	Высокий (0,2)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Y2 = 0,5 вред субъектам ПДн низкий
Кража ключей и паролей доступа внутренними и внешними нарушителями	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Высокий (0,2)	Y2 = 1,0 вред субъектам ПДн высокий
Кража, модификация, уничтожение информации	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Y2 = 0,45 вред субъектам ПДн низкий
Вывод из строя узлов ПЭВМ, каналов связи	Нулевой (0)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,2 вред субъектам ПДн нулевой
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Нулевой (0)	Средний (0,1)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Y2 = 0,35 вред субъектам ПДн низкий
Несанкционированное отключение средств защиты	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Y2 = 0,6 вред субъектам ПДн средний
Действия вредоносных программ (вирусов)	Средний (0,1)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Y2 = 0,8 вред субъектам ПДн средний
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Низкий (0,05)	Средний (0,1)	Высокий (0,2)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,45 вред субъектам ПДн низкий

Установка ПО, не связанного с исполнением служебных обязанностей	Нулевой (0)	Средний (0,1)	Нулевой (0)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,2 вред субъектам ПДн нулевой
Внедрение аппаратных закладок	Нулевой (0)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Y2 = 0,3 вред субъектам ПДн низкий
Утрата паролей доступа к ИСПДн	Низкий (0,05)	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Y2 = 0,5 вред субъектам ПДн низкий
Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкий (0,05)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,3 вред субъектам ПДн низкий
Непреднамеренное отключение средств защиты	Высокий (0,2)	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Y2 = 0,65 вред субъектам ПДн средний
Выход из строя аппаратно-программных средств	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Y2 = 0,3 вред субъектам ПДн низкий
Доступ к информации, модификация, уничтожение лиц, не допущенных к ее обработке	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Y2 = 0,9 вред субъектам ПДн средний
Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	Высокий (0,2)	Средний (0,1)	Высокий (0,2)	Высокий (0,2)	Средний (0,1)	Y2 = 0,8 вред субъектам ПДн средний
Несанкционированный доступ через ЛВС организации	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Низкий (0,05)	Y2 = 0,5 вред субъектам ПДн низкий
Перехват информации за пределами контролируемой зоны	Высокий (0,2)	Средний (0,1)	Низкий (0,05)	Средний (0,1)	Средний (0,1)	Y2 = 0,55 вред субъектам ПДн средний

Удаленный запуск приложений	Низкий (0,05)	Высокий (0,2)	Средний (0,1)	Средний (0,1)	Низкий (0,05)	Y2 = 0,5 вред субъектам ПДн низкий
Сканирование сети	Низкий (0,05)	Низкий (0,05)	Средний (0,1)	Нулевой (0)	Высокий (0,2)	Y2 = 0,4 вред субъектам ПДн низкий

Вывод:

На основании оценок, выставленных членами комиссии, данных об уровне защищенности ИСПДн МАДОУ и категориях персональных данных, обрабатываемых в них, с учетом требований, предусмотренных статьями 18.1 и 19 Федерального закона № 152-ФЗ от 27 июля 2006 г. «О персональных данных» в МАДОУ приняты следующие меры:

1. Назначен ответственный за обработку персональных данных и администратор информационных систем персональных данных;
2. Осуществляется внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных;
3. Работники, непосредственно осуществляющие обработку персональных данных, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, документами, определяющими политику организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных;
4. Разработаны правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных;
5. Обеспечивается учет машинных носителей персональных данных;
6. Обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;
7. Обеспечивается восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8. Определён перечень сотрудников, осуществляющих обработку персональных данных, сведения на бумажных носителях хранятся в сейфах или выделенных помещениях, определены места хранения персональных данных;
9. Ведётся учёт всех защищаемых носителей информации с помощью их маркировки и занесения учетных данных в журнал учета с отметкой об их выдаче (приеме);
10. Утверждены инструкции, регламентирующие работу с персональными данными и информационными системами персональных данных.
11. Перечень должностных лиц, имеющих доступ к персональным данным;
    1) Порядок доступа в помещения, где ведётся обработка персональных данных;
    2) Правила работы с обезличенными данными;
    3) Инструкция осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.
12. Исключена возможность неконтролируемого пребывания посторонних лиц в помещениях где ведется обработка персональных данных;

13. На компьютерах установлено антивирусное программное обеспечение;

14. Пользователи работают под ограниченными учетными записями;

15. Вход в информационную систему осуществляется по буквенно-цифровому паролю;

16. Используются средства резервного копирования.

Председатель комиссии:

_____

должность подпись Ф.И.О.

Члены комиссии:

_____

должность подпись Ф.И.О.

_____

должность подпись Ф.И.О.

_____

должность подпись Ф.И.О.

_____

должность подпись Ф.И.О.

«___» _____ 20_ _ года