УТВЕРЖДЕН
приказом директора МБОУ «НОШ № 5»
_____ Ким Н.А.
От 14.03.2014 № 17/1

Порядок организации и проведения работ по обеспечению информационной безопасности

Общие положения

Под организацией работ по обеспечению информационной безопасности понимается формирование совокупности мероприятий, направленных на предотвращение (нейтрализацию) угроз информационной безопасности в МБОУ «НОШ № 5» (далее – Учреждение).

Организация работ по защите информации предусматривает формирование:

- перечня конфиденциальных данных, обрабатываемых в каждой информационной системе Учреждения;
- порядка классификации информационных систем Учреждения;
- порядка разработки, ввода в действие и эксплуатации средств защиты;
- порядка взаимодействия между работниками, ответственными за обеспечение безопасности информации;
- порядка привлечения специализированных сторонних организаций к разработке и эксплуатации средств защиты, их задачи и функции на различных стадиях создания и эксплуатации информационной системы в соответствии с требованиями руководящих документов по безопасности с учетом механизмов, предусмотренных порядком размещения заказов на выполнение работ (оказание услуг) для муниципальных нужд;
- ответственности работников Учреждения за обеспечение надлежащего уровня информационной безопасности, своевременность и качество формирования требований по защите информации;
- порядка контроля за обеспечением требуемого уровня защищенности информации.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности конфиденциальных данных при их обработке в информационных системах Учреждения приказом директора Учреждения назначается ответственный за обеспечение информационной безопасности.

Для проведения классификации информационных систем Учреждения директором Учреждения создается комиссия по информационной безопасности (далее – Комиссия). В состав этой Комиссии в обязательном порядке включаются ответственный за обеспечение информационной безопасности.

В случае разработки средств защиты или ее отдельных компонентов сторонними организациями директор Учреждения отвечает за организацию и проведение мероприятий по защите информации. Разработка, внедрение и эксплуатация средств защиты информации осуществляются во взаимодействии разработчика (сторонней организацией) с ответственным за функционирование информационной системы Учреждения в технических паспортах информационных систем по прилагаемой к настоящему порядку форме № 3, для которой разрабатывалось средство защиты.

1. Определение значимости информации и классификации информационных систем

Комиссия для каждой информационной системы определяет перечень обрабатываемых конфиденциальных данных (отдельно определяет перечень

обрабатываемых ПДн), уточняет цели и основание обработки конфиденциальных данных (ПДн), а также срок хранения и условия прекращения обработки.

Целью классификации информационных систем Учреждения является определение по ее результатам перечня обоснованных организационных и технических мероприятий, позволяющих выполнить требования по обеспечению безопасности конфиденциальных данных с учетом особенностей конкретной информационной системы. Классификация может проводиться на этапе создания информационной системы или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых информационных систем).

Для информационных систем Учреждения, содержащих ПДн, при их классификации также определяется уровень защищенности ПДн. Определение уровня защищенности ПДн, обрабатываемых в ИСПДн, осуществляются Комиссией в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

Для информационных систем Учреждения класс защищенности определяется в соответствии с нормативно-правовыми актами и методическими документами ФСТЭК и ФСБ России, регулирующими деятельность в области защиты информации.

Классификация информационной системы проводится Комиссией и включает в себя следующие этапы:

- сбор и анализ исходных данных по информационной системе;

- присвоение информационной системе соответствующего класса и его документальное оформление.

В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем, если данные информационные системы не разделены между собой межсетевым экраном.

Результаты классификации информационных систем и определения уровня защищенности ПДн для ИСПДн оформляются актом (по прилагаемой к порядку форме № 1). На основании Актов заполняются технические паспорта информационных систем по прилагаемой к настоящему порядку форме № 3.

Проведение обследования информационной системы может осуществляться как системный администратором, так и специалистами сторонних организаций, имеющих соответствующие лицензии на деятельность по технической защите информации, на договорной основе.

Класс информационной системы может быть пересмотрен Комиссией в следующих случаях:

- на основании результатов проведенного анализа и оценки угроз безопасности конфиденциальных данных с учетом особенностей и (или) изменений конкретной информационной системы;

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности конфиденциальных данных, при их обработке в информационной системе.

Форма № 1

АКТ
классификации информационной системы
(определения уровня защищенности ПДн, обрабатываемых в ИСПДн)
«Сетевой город. Образование», «Кадры»

Исходные данные информационной системы

Уровень значимости информации	УЗ -3
Категория персональных данных	общедоступные
Актуальность угрозы безопасности	Угрозы 3-го типа
Объем обрабатываемых данных	В информационной системе одновременно обрабатываются данные менее чем 100000
Масштаб информационной системы	объектовый

Комиссия в составе:
председателя ___ _____

членов комиссии: _____,

рассмотрев исходные данные на информационную систему
«Сетевой город. Образование», «Кадры»
в соответствии с нормативно-правовыми актами и методическими документами ФСТЭК и ФСБ России, регламентирующими деятельность в области защиты информации,

Решила:

Установить ИС АИС «Сетевой город. Образование», «Кадры»
Класс защищенности ИС К-3
Уровень защищенности ПДн УЗ-3

Председатель комиссии _____ _____
(подпись) (ФИО)

Члены комиссии: _____ _____
_____ _____
_____ _____
«___» _____ 20__ г.

Форма № 2

Технический паспорт
информационной системы
«АИС «Сетевой город. Образование», «Кадры»»

1. Общие сведения об ИС.
1.1. Наименование ИС: «АИС «Сетевой город. Образование», «Кадры»».
1.2. Физическое расположение ИС: МБОУ «НОШ № 5»
1.3. Класс ИС: К- 3 (акт классификации ИС от ____.20__ г).
1.4. Перечень конфиденциальных данных, обрабатываемых в ИС (Таблица 1)

Таблица 1

ПЕРЕЧЕНЬ
конфиденциальных данных, обрабатываемых в ИС

№ п/п	Наименование конфиденциальных данных	Категория	Цель обработки ПДн в рамках ИСПДн
1	Ф.И.О учащихся и работников		
2	Дата рождения		

2. Технологические процессы обработки ПДн, используемые в ИСПДн (Таблица 2).

Таблица 2

ПЕРЕЧЕНЬ
технологических процессов обработки конфиденциальных данных,
используемых в ИС

№ п/п	Наименование технологического процесса
1	Внесение ПДн
2	Изменение
3	Удаление
4	Подготовка отчётов

3. Состав оборудования ИС.
3.1. Состав основных технических средств и систем (ОТСС) (Таблица 3):

Таблица 3

ПЕРЕЧЕНЬ
основных технических средств и систем, входящих в состав ИС

№ п/п	Тип ОТСС	Программные и технические характеристики	Место установки	Кол-во, штук
1	Персональный компьютер		Кабинет директора	2
2	Персональные компьютеры		Классные кабинеты	9

3.2. Состав вспомогательных технических средств и систем (ВТСС) (Таблица 4):

Таблица 4

ПЕРЕЧЕНЬ
вспомогательных технических средств, входящих в состав ИС «АИС «Сетевой город. Образование», «Кадры»
(средств вычислительной техники, не участвующих в обработке информации)

№ п/п	Наименование и тип ВТСС	Место установки	Кол-во, штук	Примечание
1	МФУ	Кабинет директора	2	
2	МФУ	Классный кабинет	3	

3.3. Состав систем защиты информации приведены в Таблице 5.

Таблица 5

ПЕРЕЧЕНЬ
систем защиты информации,
установленных в ИС «АИС «Сетевой город. Образование», «Кадры»

№ п/п	Наименование и тип технического средства	Сведения о сертификате	Место установки
1	Антивирус «Аваст»	Бесплатная версия сроком на 1 год	Каб № 1, 2,5,7,8, 9,10 Кабинет директора
2	Антивирус «Касперский»	коммерческая лицензия срок с 12.08.2013 по 07.07.2014	Каб № 3, 6
3	Сертификат Inside Systems	действие с 20.03.2014 по 04.08.2041	Во всех классных кабинетах, в кабинете директора, у секретаря

Председатель комиссии _____ _____
(подпись) (ФИО)

Члены комиссии: _____ _____
(подпись) (ФИО)

_____ _____
(подпись) (ФИО)