Утверждаю
Заведующий МБДОУ «Ромашка»
_____ Егорова И.В.
«01» 09 2017 г.

ПОЛОЖЕНИЕ
по организации контроля эффективности защиты информации Муниципального бюджетного дошкольного образовательного учреждения «Ромашка» муниципального образования город Ноябрьск

1. Общие положения

1.1. Положение по организации контроля эффективности защиты информации (далее – Положение) разработано в соответствии с «Положением по организации и проведению работ по обеспечению информационной безопасности» при ее обработке в информационных системах (далее – информационная система) *Муниципального бюджетного дошкольного образовательного учреждения «Ромашка» муниципального образования город Ноябрьск* (далее – Организация).

1.2. Положение разработано в целях контроля реализации принятых мер по обеспечению безопасности конфиденциальной информации в Организации.

1.3. Положение определяет основные мероприятия по контролю эффективности принятых мер по обеспечению безопасности конфиденциальной информации при ее обработке в информационной системе Организации.

2. Общий порядок организации контроля эффективности мер защиты информации

2.1. Ответственным за контроль эффективности защиты конфиденциальной информации является ответственный за защиту информации.

2.2. Администратор безопасности информации Организации осуществляет постоянный контроль выполнения требований по обеспечению безопасности информации в рамках выполнения своих обязанностей.

2.3. Мероприятия по контролю эффективности принятых мер по обеспечению безопасности информации при ее обработке в информационной системе Организации должны включать:

- создание комиссии по контролю исполнения мероприятий по защите информации;
- установление порядка проведения внутренних проверок состояния защиты информации.

2.4. Состав комиссии по контролю состояния защиты информации утверждается ответственным за обеспечение безопасности информации.

3. Порядок проведения внутренних плановых проверок состояния защиты информации

3.1. Внутренние проверки состояния защиты информации при ее обработке в информационной системе Организации проводятся в соответствии с Планом внутренних проверок состояния защиты информации (Приложение № 1).

3.2. План внутренних проверок состояния защиты информации составляется на год ответственным за защиту информации и утверждается руководителем Организации.

3.3. Руководители подразделений, работники которых осуществляют обработку конфиденциальной информации, должны обеспечивать возможность проведения внутренних проверок состояния защиты информации.

3.4. Внутренние проверки состояния защиты информации должны проводиться не реже одного раза в три года.

3.5. Проверками должны быть охвачены все подразделения Организации, работники которых осуществляют обработку конфиденциальной информации.

3.6. При проведении внутренних проверок состояния защиты информации должен присутствовать представитель проверяемого подразделения.

3.7. Необходимыми видами внутренних проверок состояния защиты информации являются проверки выполнения требований к организации:

- системы допуска и учета лиц, допущенных к работе с конфиденциальной информацией;
- системы защиты межсетевого взаимодействия;
- режима безопасности помещений информационной системы, в которой осуществляется обработка конфиденциальной информации;
- безопасного хранения и уничтожения материальных носителей информации;
- защиты от вредоносного кода;
- парольной защиты;
- управления инцидентами информационной безопасности и реагирование на них;
- управления конфигурацией информационной системы Организации и системы защиты информации;
- системы криптографической защиты информации;
- системы резервного копирования и восстановления;
- системы обучения по вопросам обеспечения безопасности информации.

3.8. Обо всех существенных нарушениях, выявленных в ходе проведения внутренних проверок состояния защиты информации незамедлительно сообщается руководителю Организации.

3.9. По фактам выявленных нарушений проводятся служебные расследования в соответствии с порядком, определенном в «Положении о выявлении и реагировании на инциденты информационно безопасности».

3.10. Обязанности по проведению разбирательств по выявленным фактам несоблюдения требований по информационной безопасности, которые могут привести к снижению уровня защищенности информации, возложены на администратора безопасности информации.

3.11. По результатам проведения проверки каждого подразделения комиссией по контролю состояния защиты информации составляется Отчет по результатам проведения проверки (Приложение № 2). Отчет по результатам проведения проверки согласуется с руководителем проверяемого структурного подразделения Организации и предоставляется на утверждение руководителю Организации ответственным за защиту информации.

3.12. Проведенные внутренние проверки должны учитываться в Журнале учета проводимых внутренних проверок ответственным за защиту информации (Приложение № 3).

Приложение №1
к положению об организации
контроля эффективности

ФОРМА

Плана внутренних проверок состояния защиты конфиденциальной информации
Организации на 20__ г.

№ п/п	Структурное подразделение	Период проведения внутренних проверок
1.		
2.		
3.		
	....	

Руководитель _____ _____

(м.п.) (инициалы, фамилия)

«___» _____20_ г.

Приложение №2
к положению об организации
контроля эффективности

ФОРМА

Отчета о проведении проверки контроля эффективности защиты информации

Для оценки выполнения требований по защите конфиденциальной информации в период _____ была проведена проверка отдела _____.

Результаты внутренней проверки состояния защиты конфиденциальной информации приведены в таблице 1.

Таблица 1 – Результаты внутренней проверки состояния защиты конфиденциальной информации

№ п/п	Вид внутренней проверки	Выявленные нарушения	Корректирующие меры
1	Организация системы допуска и учета лиц, допущенных к конфиденциальной информации		
2	Организация системы защиты межсетевого взаимодействия		
3	Организация режима безопасности помещений информационных систем		
4	Организация безопасного хранения и уничтожения материальных носителей информации		
5	Организация защиты от вредоносного кода		
6	Организация парольной защиты		
7	Организация управления инцидентами информационной безопасности и реагирование на них		
8	Организация управления конфигурацией информационных систем Организации и системы защиты конфиденциальной информации		
9	Организация системы криптографической защиты информации		
10	Организация системы резервного копирования и восстановления		
11	Организации централизованного управления системой защиты информации		
12	Организация системы обучения по вопросам обеспечения безопасности информации		

Руководителю отдела _____ в срок до _____ устранить выявленные в ходе проверки недочеты и составить отчет по итогам работы на имя руководителя Организации.

Ответственный за обеспечение безопасности конфиденциальной информации _____/_____/

«____» _____ 20___г.

ОЗНАКОМЛЕН

_____ _____/_____/

«____» _____ 20___г.

Регистрационный номер_____

Приложение №3
к положению об организации
контроля эффективности

ЖУРНАЛ УЧЕТА ПРОВОДИМЫХ ВНУТРЕННИХ ПРОВЕРОК

Начат «___»_____20__ г.

Окончен «___»_____20__ г.

На _____листах

_____	_____	_____
(должность руководителя)	(подпись) М.П.	(Фамилия И.О.)

Журнал учета проводимых внутренних проверок стр._____

№ п/п	Наименование внутренней проверки	Краткое описание	Дата проведения проверки	Подпись ответственного за контроль эффективности мер по защите информации	Примечание
1	2	3	4	5	6