

Инструкция №15

по порядку контроля за обеспечением уровня защищенности информации в информационной системе МБДОУ «Вагановский д/с»

1. Общие положения

1.1. Настоящая Инструкция по порядку контроля за обеспечением уровня защищенности информации в информационной системе «МБДОУ «Вагановский д/с»(далее – Инструкция) определяет правила и процедуры контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе«МБДОУ «Вагановский д/с»(далее – ИС).

1.2. В ходе контроля за обеспечением уровня защищенности информации, содержащейся в ИС, осуществляются:

- контроль (анализ) защищенности информации с учетом особенностей функционирования ИС;
- анализ и оценка функционирования ИС и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации ИС;
- документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в ИС;
- принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в ИС, о необходимости доработки (модернизации) ее системы защиты информации.

1.3. Контроль за обеспечением уровня защищенности информации, содержащейся в ИС, проводится «МБДОУ «Вагановский д/с» самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

2. Оформление результатов контрольных мероприятий

2.1. По итогам проведения контрольных мероприятий лицо (комиссия)разрабатывает отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- заключение по итогам проведения внутреннего контрольного мероприятия.

2.2. Отчет передается на рассмотрение руководству «МБДОУ «Вагановский д/с».

2.3. Результаты проведения мероприятий заносятся в Протокол проведения контроля за обеспечением уровня защищенности информации в ИС(Приложение № 1).

3. Порядок проведения контрольных мероприятий

3.1. Контрольные мероприятия проводятся при обязательном участии ответственного за защиту информации в ИС, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администратор безопасности ИС и системный администратор ИС.

3.2. При проведении контрольных мероприятий администратор безопасности ИС проводит анализ уязвимостей с использованием сертифицированных по требованиям безопасности средств анализа защищенности.

3.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий должны быть полностью, объективно и всесторонне установлены:

- соблюдение принципов обработки защищаемой информации;
- соответствие полномочий пользователей правилам доступа;
- выполнение всеми работниками требований и правил обработки защищаемой информации в ИС;
- соблюдение пользователями требований парольной и антивирусной защиты;
- соблюдение администраторами ИС инструкций и регламентов по обеспечению безопасности информации;
- соблюдение порядка доступа в помещения;
- знание пользователями положений инструкций, в части их касающейся;
- актуальность перечня информационных систем и защищаемой информации;
- порядок и условия применения СЗИ;
- состояние учета машинных носителей информации;
- наличие (отсутствие) фактов несанкционированного доступа к защищаемой информации и принятие необходимых мер;
- осуществление мероприятий по обеспечению целостности защищаемой информации;
- проведенные мероприятия по восстановлению защищаемой информации, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- технические мероприятия, связанные со штатным и нештатным функционированием СЗИ;
- технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации.

3.4. При выявлении в ходе проверки нарушений в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

3.5. Протоколы хранятся у ответственного за защиту информации в ИС. Уничтожение протоколов проводится ответственным за защиту информации в ИС самостоятельно в январе года следующего за проверочным годом. При необходимости протоколы могут храниться до полного устранения нарушений.

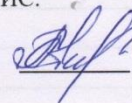
3.6. О результатах проверки и мерах, необходимых для устранения нарушений, руководству «МБДОУ «Вагановский д/с» докладывает ответственный за защиту информации в ИС.

3.7. По результатам проверки в случае необходимости принимается решение о необходимости доработки (модернизации) системы защиты информации.

4. Ответственность

4.1. За организацию проведения проверок по контролю за обеспечением уровня защищенности информации отвечает ответственный за защиту информации в ИС.

Разработчик инструкции заведующий детским садом С.Л. Савченко



Лист ознакомления с инструкцией
по порядку контроля за обеспечением уровня защищенности информации в
информационной системе «МБДОУ «Вагановский д/с».

№ п/п	Ф.И.О. работника	Дата ознакомления	Личная подпись
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			
29			
30			

ПРОТОКОЛ № _____
проведения контрольных мероприятий по обеспечению уровня защищенности
информации в информационной системе
МБДОУ «Вагановский д/с».

Настоящий Протокол составлен в том, что « _____ » _____ 20__ г.
_____ (комиссией)

[Должность, Ф.И.О. работника]

проведена проверка _____
[Тема проверки]

Проверка осуществлялась в соответствии с требованиями:

[Название документа]

В ходе проверки проверено:

Выявленные нарушения:

Меры по устранению нарушений:

Срок устранения нарушений: _____

Председатель комиссии:

[Наименование должности]	[Личная подпись]	[Расшифровка подписи — инициалы, фамилия]
--------------------------	------------------	---

Члены комиссии:

[Наименование должности]	[Личная подпись]	[Расшифровка подписи — инициалы, фамилия]
--------------------------	------------------	---

[Наименование должности]	[Личная подпись]	[Расшифровка подписи — инициалы, фамилия]
--------------------------	------------------	---

[Наименование должности]	[Личная подпись]	[Расшифровка подписи — инициалы, фамилия]
--------------------------	------------------	---

[Наименование должности руководителя проверяемого подразделения]	[Личная подпись]	[Расшифровка подписи — инициалы, фамилия]
---	------------------	---