

ПРИКАЗ

30.11.2023 г.

№ 486

***Об утверждении Положения о внутреннем аудите
соответствия обработки персональных данных
Федеральному закону от 27.07.2006 № 152-ФЗ
«О персональных данных» и, принятыми
в соответствии с ним, нормативными
правовыми актами Российской Федерации***

С целью исполнения требований Федерального закона от 27.07.2006 № 152-ФЗ
«О персональных данных»

ПРИКАЗЫВАЮ:

1. Считать утратившим силу приказ от 24.05.2021 г. №144 «Об утверждении Положения о внутреннем аудите соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и, принятыми в соответствии с ним, нормативными правовыми актами РФ»;
2. Утвердить и ввести в действие с «30» ноября 2023 г Положение о внутреннем аудите соответствия обработки персональных данных в ГБОУ РК «Феодосийская санаторная школа-интернат» Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и, принятыми в соответствии с ним, нормативными правовыми актами Российской Федерации (Приложение №1).
3. Утвердить состав комиссии по проведению внутреннего аудита соответствия обработки персональных данных в ГБОУ РК «Феодосийская санаторная школа-интернат» (Приложение №2).
4. Секретарю руководителя Багировой А.З. ознакомить сотрудников, допущенных к обработке персональных данных, с перечнем мест хранения.
5. Инженеру-программисту Калачикову А.В. разместить настоящее Положение на официальном сайте ГБОУ РК «Феодосийская санаторная школа-интернат» в сети Интернет.
6. Контроль за исполнением настоящего приказа оставляю за собой.

Директор

И.В.Калинина

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00f6f8e4f7a627a92bac75623911e578bb
Владелец: Калинина Ирина Васильевна
Дата подписи: 04.12.23 08:51
Действителен: с 2023-05-04 до 2024-07-27

ПОЛОЖЕНИЕ
о внутреннем аудите соответствия обработки персональных данных
в ГБОУ РК «Феодосийская санаторная школа-интернат» Федеральному закону
от 27.07.2006 № 152-ФЗ «О персональных данных» и, принятыми в соответствии с
ним, нормативными правовыми актами Российской Федерации

1. Настоящее Положение определяет процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок проведения внутреннего контроля соответствия обработки персональных данных в структурных подразделениях ГБОУ РК «Феодосийская санаторная школа-интернат» (далее — Школа-интернат) требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (далее — Федеральный закон «О персональных данных»), принятыми в соответствии с ним правовыми актами.

2. Настоящее Положение разработано в соответствии с Федеральным законом «О персональных данных», постановлениями Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и принятыми в соответствии с ними нормативными правовыми актами.

3. В настоящем Положении используются основные понятия в значениях, определенных статьей 3 Федерального закона «О персональных данных».

4. Внутренний аудит соответствия обработки персональных данных в структурных подразделениях Школы-интернат требованиям к защите персональных данных (далее — внутренний аудит) осуществляется комиссией по проведению внутреннего контроля соответствия обработки персональных данных в структурных подразделениях Школы-интернат требованиям к защите персональных данных (далее — комиссия) путем проведения проверок. Состав комиссии утверждается приказом директора Школы-интернат.

5. Проверки по предметам контроля, указанным в акте внутреннего аудита, согласно приложению №1 к настоящим Правилам, могут осуществляться как непосредственно на рабочих местах исполнителей, участвующих в обработке персональных данных, так и путем направления запросов и рассмотрения документов, необходимых для осуществления внутреннего контроля.

6. Проверки соответствия обработки персональных данных, установленных требованиям, проводятся один раз в год в каждом структурном подразделении Школы-интернат.

6.1. Проведение внеплановой проверки организуется в течение трех рабочих дней.

7. План проведения внутреннего контроля на очередной год формируется ответственным за обработку персональных данных до 15 декабря и утверждается директором (приложения №2,3).

8. Утвержденный план очередности проведения внутреннего контроля доводится до структурных подразделений школы-интернат.

9. Проведение внеплановой проверки организуется председателем комиссии, а в его отсутствие — заместителем председателя комиссии в течение трех рабочих дней с даты поступления письменного заявления субъекта персональных данных о нарушении правил обработки персональных данных.

9.1. Внеплановые контрольные мероприятия проводятся на основании решения комиссии. Решение о проведении внеплановых контрольных мероприятий может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности;
- по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению руководителя Школы-интернат.

9.2. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению мер безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
- состояние учета машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

10. Комиссия при проведении внутреннего контроля имеет право:

- запрашивать у руководителей структурных подразделений Школы-интернат информацию и (или) документы, необходимые для осуществления внутреннего аудита;
- требовать у ответственных за обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

11. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего аудита, должна обеспечиваться конфиденциальность.

12. Мероприятие внутреннего контроля не может длиться больше 10 рабочих дней с даты начала проверки.

13. Результаты проведенных проверок оформляются секретарем комиссии в виде акта внутреннего аудита, составленного по форме согласно Приложению №1 к настоящему Положению, который подписывается членами комиссии в количестве не менее трех человек и утверждается председателем комиссии, а в его отсутствие — заместителем председателя комиссии.

14. О результатах внутреннего контроля и мерах, необходимых для устранения выявленных нарушений, по мере необходимости председатель комиссии докладывает на очередном совещании при директоре Школы-интернат.

Приложение №1 к Положению
о внутреннем аудите соответствия
обработки персональных данных

АКТ

**внутреннего аудита соответствия обработки персональных данных
в ГБОУ РК «Феодосийская санаторная школа-интернат»
требованиям к защите персональных данных**

Настоящий Акт составлен в том, что «___»_____ 20__года комиссией по проведению
внутреннего аудита соответствия обработки персональных данных в ГБОУ РК
«Феодосийская санаторная школа-интернат» проведена проверка

(тема проверки)

Проверка осуществлялась в соответствии с требованиями

(наименование документа)

Проверено:

Выявленные нарушения:

Меры по устранению нарушений:

Срок устранения нарушений:_____.

Председатель комиссии _____(_____)

Члены комиссии: _____(_____)
_____ (_____)

Секретарь комиссии _____(_____)

ПЛАН-ГРАФИК
внутренних проверок контроля соответствия обработки персональных данных
требованиям к защите персональных данных

[illegible]

ПЛАН
внутренних внеплановых проверок контроля соответствия обработки
персональных данных требованиям к защите персональных данных

№	Тема проверки	Нормативный правовой документ предъявляющий требования	Срок проведения	Исполнитель
1.	Соответствие полномочий пользователя разрешительной системе доступа	Разрешительная система доступа		
2.	Соблюдение пользователями информационных систем персональных данных парольной политики	Инструкция пользователя		
3.	Соблюдение пользователями информационных систем персональных данных антивирусной политики	Инструкция по антивирусной защите		
4.	Соблюдение пользователями информационных систем персональных данных правил работы со съёмными носителями персональных данных	Инструкция по работе со съёмными носителями		
5.	Соблюдение правил работы с средствами криптографической защиты	Инструкции по работе со средствами криптографической защиты		
6.	Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных	Порядок доступа сотрудников в помещения, где ведется обработка персональных данных		
7.	Соблюдение порядка резервирования баз данных и хранения	Инструкция о порядке резервирования и восстановления		

	резервных копий	работоспособности технических средств программного обеспечения и баз данных		
8.	Соблюдение порядка работы со средствами защиты информации	Инструкция пользователя информационных систем персональных данных, инструкция администратора информационных систем персональных данных по обеспечению безопасности персональных данных		
9.	Соблюдение правил хранения и работы с бумажными носителями персональных данных	Инструкция по порядку учета и хранения документов, содержащих персональные данные		

Комиссия
по проведению внутреннего аудита соответствия обработки
персональных данных в ГБОУ РК «Феодосийская санаторная школа-интернат»

№	Полномочия	ФИО	Должность
1.	Председатель комиссии	Купцова В.П.	Заместитель директора по УР
2.	Члены комиссии	Рак О.Н.	Главный бухгалтер
3.		Калачиков А.В.	Инженер-программист
4.	Секретарь комиссии	Багирова А.З.	Секретарь руководителя