

Приложение №11
к приказу
МАОУ «Лицей №1»
от 19.05.2020 № 166

УТВЕРЖДАЮ
Директор МАОУ «Лицей №1»
Полонская Н.А.
«19» мая 2020 г.



ПРАВИЛА

проведения внутреннего контроля и проверок соответствия обработки персональных данных требованиям к защите персональных данных в МАОУ «Лицей №1» г. Сыктывкара

1. Настоящими Правилами осуществления внутреннего контроля (далее – Проверочные мероприятия) и проверок соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в МАОУ «Лицей №1» определяются процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Настоящие Правила разработаны в соответствии с:

- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- постановлением Правительства Российской Федерации от 15.сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации»;
- постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О

персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

– приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. В настоящих Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в МАОУ «Лицей №1» организовывается проведение периодических проверок условий обработки персональных данных.

5. Проверочные мероприятия осуществляются ответственным за организацию обработки персональных данных МАОУ «Лицей №1».

6. Проверочные мероприятия могут быть плановыми и внеплановыми.

7. Проведение плановых Проверочных мероприятий осуществляется в соответствии с ежегодным планом внутренних проверок.

8. Ежегодный план проверок (приложение 1) утверждается директором МАОУ «Лицей №1» ежегодно по окончании календарного года.

9. Проведение внеплановых Проверочных мероприятий осуществляется по распоряжению директора «МАОУ «Лицей №1».

10. Проведение внеплановых Проверочных мероприятий организуется в течение трех рабочих дней с момента распоряжения директора МАОУ «Лицей №1».

11. При проведении Проверочных мероприятий соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

– порядок и условия применения организационных и технических мер по обеспечению 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.

12. По результатам Проверочных мероприятий готовятся акты проверок.

13. Ответственный за организацию обработки персональных данных имеет право:

– запрашивать у сотрудников МАОУ «Лицей №1» информацию, необходимую для реализации полномочий;

– 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.

14. Проверочные мероприятия должны быть завершены не позднее чем через месяц со дня принятия решения о её проведении. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, директору МАОУ «Лицей №1» докладывает ответственный за организацию обработки персональных данных.

Приложение 1
к Правилам проведения внутреннего контроля и
проверок соответствия обработки персональных
данных требованиям к защите персональных
данных в МАОУ «Лицей №1»
(форма)

УТВЕРЖДАЮ
Директор МАОУ «Лицей №1»
_____/Полонская Н.А.
« ____ » _____ 20__ г.

ПЛАН

мероприятий по обеспечению безопасности персональных данных на 20__ год в МАОУ «Лицей №1»

1. План мероприятий по обеспечению безопасности персональных данных на 2019 год в МАОУ «Лицей №1» (далее – План) разработан во исполнение требований статьи 18.1. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», с целью обеспечения выполнения требований законодательства Российской Федерации по защите персональных данных в МАОУ «Лицей №1», а также контроля актуализации установленных мер и реализованных мероприятий, обеспечивающих исполнение указанных требований.

2. При изменении условий режима защиты персональных данных, структуры или принципов функционирования системы защиты персональных данных, соответствующие изменения должны быть отражены в настоящем плане в виде корректировок или добавления новых мероприятий.

3. Все внесенные изменения утверждаются директором МАОУ «Лицей №1».

4. План утверждается ежегодно в конце текущего года на следующий календарный год.

5. План внутренних проверок (таблица № 1) распространяется на все информационные системы персональных данных МАОУ «Лицей №1».

6. Оригинал плана хранится у ответственного лица за организацию обработки персональных данных в МАОУ «Лицей №1».

**Таблица 1 – План мероприятий по обеспечению безопасности персональных данных в
МАОУ «Лицей №1»**

№	Мероприятие	Срок выполнения	Исполнитель	Результат	Примечание
1.	Назначение ответственного за организацию обработки персональных данных	при смене ответственного лица	Ответственный за организацию обработки ПДн		
2.	Актуализация и разработка организационно-распорядительных документов по обеспечению безопасности персональных данных	декабрь 2019	Ответственный за организацию обработки ПДн		
3.	Организация получения согласий на обработку персональных данных	при необходимости, при принятии новых сотрудников	Ответственный за организацию обработки ПДн		
4.	Ознакомление работников с локально-нормативными актами в области защиты информации	при необходимости, при принятии новых сотрудников	Ответственный за организацию обработки ПДн		
5.	Учет сейфов и ключей от них, шкафов, где хранятся	ежеквартально	Ответственный за организацию обработки ПДн		

№	Мероприятие	Срок выполнения	Исполнитель	Результат	Примечание
	персональные данные				
6.	Определение функций, обязанностей и ответственности пользователей ИСПДн	при изменении, декабрь 2019 (актуализация)	Ответственный за организацию обработки ПДн		
7.	Определение перечня прав доступа к ресурсам ИСПДн	при изменении, декабрь 2019 (актуализация)	Ответственный за организацию обработки ПДн		
8.	Определение мест хранения ПДн и их материальных носителей	при изменении, ежеквартально (актуализация)	Ответственный за организацию обработки ПДн		
9.	Организация порядка резервного копирования	при изменении	Ответственный за организацию обработки ПДн		
10.	Актуализация должностных инструкций работников, обрабатывающих ПДн	при необходимости	Ответственный за организацию обработки ПДн		
11.	Расположение АРМ ИСПДн таким образом, чтобы исключалась возможность просмотра информации с мониторов АРМ	при необходимости	Ответственный за организацию обработки ПДн		

№	Мероприятие	Срок выполнения	Исполнитель	Результат	Примечание
	посторонними лицами и техническими средствами				
12.	Оснащение помещений, предназначенных для обработки персональных данных запираемыми шкафами, столами, сейфами для хранения материальных носителей ПДн	при необходимости, в течение года	Ответственный за организацию обработки ПДн		
13.	Внедрение резервных (дублирующих) технических средств ключевых элементов	при необходимости	Ответственный за организацию обработки ПДн		
14.	Организация порядка восстановления работоспособности технических средств ПО, баз данных с подсистем системы защиты ПДн	постоянно	Ответственный за организацию обработки ПДн		
15.	Контроль за соблюдением	ежемесячно	Ответственный за организацию		

№	Мероприятие	Срок выполнения	Исполнитель	Результат	Примечание
	режима защиты ПДн		обработки ПДн в подразделениях		
16.	Контроль за обработкой ПДн	ежемесячно	Ответственный за организацию обработки ПДн в подразделениях		
17.	Контроль за уничтожением ПДн и их материальных носителей	ежеквартально	Ответственный за организацию обработки ПДн		
18.	Контроль за исполнением обращений субъектов ПДн (запросов)	ежемесячно	Ответственный за организацию обработки ПДн		
19.	Контроль за исполнением плана резервного копирования	постоянно согласно Регламенту резервного копирования	Ответственный за организацию обработки ПДн		
20.	Проведение внутренних проверок условий обработки и защиты ПДн и выполнения требований законодательства РФ	ежегодно	Ответственный за организацию обработки ПДн в соответствии с Планом утверждается ежегодно в декабре.		
21.	Проверка наличия материальных носителей ПДн (документов на	ежегодно	Ответственный за организацию обработки ПДн		

№	Мероприятие	Срок выполнения	Исполнитель	Результат	Примечание
	бумажных носителях и МНИ)				
22.	Контроль за ведением журналов	раз в 6 месяцев	Ответственное лицо назначенные приказом за ведение журналов		
23.	Разработка и внедрение системы проверки знаний работников условий обработки и защиты П/Дн и выполнения требований законодательства РФ	2 кв. 2019 г.	Ответственный за организацию обработки персональных данных		
24.	Проведение инструктажа работников по условиям обработки и защиты П/Дн и выполнения требований законодательства РФ. Проверка знаний (Проведение тестирования)	3 кв. 2019 г.	Ответственный за организацию обработки персональных данных		

ЛИСТ ОЗНАКОМЛЕНИЯ
с Правилами проведения внутреннего контроля и проверок соответствия
обработки персональных данных требованиям к защите персональных
данных в МАОУ «Лицей №1» г. Сыктывкара

с Правилами проведения внутреннего контроля и проверок соответствия обработки персональных данных требованиям к защите персональных данных в МАОУ «Лицей №1» г. Сыктывкара

[illegible]