

Согласовано:
Председатель ПК
Лобкова Е.В.

Утверждаю:
Директор школы:
Г.В. Кряжова



Приказ №40/1 от 05.04.2017

**Правила
осуществления внутреннего контроля соответствия обработки персональных дан-
ных требованиям к защите персональных данных,
установленным Федеральным законом «О персональных данных», принятыми в
соответствии с ним правовыми актами МОУ Кренёвской СОШ**

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила разработаны в соответствии Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), постановлением Правительства Российской Федерации от 21 марта 2012 года № 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» и определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, основания и порядок проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом № 152-ФЗ, принятыми в соответствии с ним правовыми актами МОУ Кренёвской СОШ (далее – внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных).

II. УСЛОВИЯ ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в МОУ Кренёвской СОШ организовывается проведение периодических проверок условий обработки персональных данных (далее - проверки).

2.2. Проверки осуществляются должностным лицом, ответственным за организацию обработки персональных данных в МОУ «Кренёвская СОШ (далее - ответственный за организацию обработки персональных данных), либо комиссией, образуемой правовым актом МОУ Кренёвской СОШ.

2.3. В проведении проверки не может участвовать сотрудник МОУ Кренёвской СОШ прямо или косвенно заинтересованный в её результатах.

2.4. Проверки проводятся на основании утвержденного в МОУ Кренёвской СОШ ежегодного Плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных (плановые проверки) или на основании поступившего в МОУ Кренёвской СОШ письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки) (Приложение 1)

2.5. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн.

2.6. Плановые проверки проводятся не чаще чем один раз в полгода.

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

2.8. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении плановых 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 образовательного учреждения.

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

2.9.1. 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;

2.9.2. порядок и условия применения средств защиты информации;

2.9.3. эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

2.9.4. состояние учета машинных носителей персональных данных;

2.9.5. соблюдение правил доступа к персональным данным;

2.9.6. наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

2.9.7. мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

2.9.8. осуществление мероприятий по обеспечению целостности персональных данных.

2.10. Ответственный за организацию обработки персональных данных в МОУ Кренёвской СОШ или комиссия имеет право:

2.10.1. запрашивать у сотрудников в МОУ Кренёвской СОШ информацию, необходимую для реализации полномочий;

2.10.2. требовать от уполномоченных на обработку персональных данных должностных лиц в МОУ Кренёвской СОШ уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

2.10.3. принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства РФ;

2.10.4. вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

2.10.5. вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства РФ в отношении обработки персональных данных.

2.11. В отношении персональных данных, ставших известными ответственному за организацию обработки персональных данных, либо комиссии в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

2.12. По результатам проведения проверки оформляется протокол проверки (приложение 2), результаты проверок фиксируются в журнале (приложение 4). Протокол подписывается ответственным за организацию обработки ПД или членами комиссии.

2.13. При выявлении нарушений в сфере защиты персональных данных составляется акт (приложение 3), выявленные нарушения фиксируются в журнале (приложение 4).

2.14. Срок проведения проверки и оформления акта составляет 30 календарных дней со дня начала проверки, указанного в правовом акте о назначении проверки.

2.15. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывает ответственный за организацию обработки персональных данных либо председатель комиссии, в форме письменного заключения.

2.16. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий должно быть уведомлено о проведении проверки и ознакомлено с Планом проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

Приложение 1
к Правилам осуществления внутреннего
контроля соответствия обработки
персональных данных требованиям
к защите персональных данных

ПЛАН

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

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности ПД
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности ПД
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности ПД
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности ПД
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности ПД
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн		Ежемесячно	Ответственный за обеспечение безопасности ПДн
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС СПО	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности ПДн
Контроль обеспечения резервного копирования		Ежемесячно	Ответственный за обеспечение безопасности ПДн
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а		Ежегодно	Ответственный за обеспечение

также предсказание появления новых, еще неизвестных, угроз			безопасности ПДн
Поддержание в актуальном состоянии нормативно-организационных документов		Ежемесячно	Ответственный за организацию обработки ПДн
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	Ответственный за организацию обработки ПДн

Приложение 2
к Правилам осуществления внутреннего
контроля соответствия обработки персональных
данных требованиям к защите персональных данных

ПРОТОКОЛ № ____

проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в МОУ Кренёвской СОШ

Настоящий Протокол составлен в том, что «__»_____20__ г.
_____ (комиссией)

(должность, Ф.И.О. сотрудника)

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:

фамилия и инициалы / подпись / должность

Члены комиссии:

фамилия и инициалы / подпись / должность
фамилия и инициалы / подпись / должность

Приложение 3
к Правилам осуществления внутреннего
контроля соответствия обработки персональных
данных требованиям к защите персональных данных

А К Т №

выявления нарушений в сфере защиты персональных данных и иной конфиденциальной информации

20____
г

Настоящий акт составлен в том, что в

(наименование структурного подразделения, где выявлено нарушение)

ФИО и должность лица, допустившего нарушение _____
допущено нарушение установленных требований в сфере защиты персональных данных и иной конфиденциальной информации.

Содержание нарушения _____

Требования каких нормативных документов нарушены _____

Комиссия (или уполномоченное лицо), выявившая нарушения

Подписи

(подпись)

(Ф. И. О.)

(подпись)

(Ф. И. О.)

(подпись)

(Ф. И. О.)

С актом ознакомлены:

подпись лица, допустившего нарушение _____ (ФИО _____)

подпись руководителя структурного подразделения, где допущено нарушение _____ (ФИО _____)

Приложение 4
к Правилам осуществления внутреннего
контроля соответствия обработки персональных
данных требованиям к защите персональных данных

ЖУРНАЛ
регистрации выявленных нарушений в сфере защиты персональных данных и
иной конфиденциальной информации

Начат «__» _____ 20__ г.
Окончен «__» _____ 20__ г.

№	Дата выявления нарушения	Подразделение, где выявлено нару- шение и допустив- шее нарушение лицо (ФИО, должность)	Кем и при каких обстоятельствах выявлено наруше- ние (жалоба, пла- новая проверка и т.д.)	Со- держа- ние нару- шения	Требования, каких норматив- ных документов нарушены	Кор- ректи- рую- щие и преду- пре- ждаю- щие дей- ствия по устра- нению нару- шения и предот- враще- нию нару- шения в даль- ней- шем	От- вет- ствен- ное за устра- нение лицо выяв- лен- ного нару- шения лицо (ФИО, долж- ность и его под- пись	Срок устра- нения нару- шения	От- метка о кон- троле за вы- полне- нием (дата, ФИО и долж- ность прове- ряю- щего
1	2	3	4	5	6	7	8	9	10

ЖУРНАЛ
регистрации проверок в сфере защиты персональных данных и иной конфиденци-
альной информации

Начат «__» _____ 20__ г.
Окончен «__» _____ 20__ г.

№	Дата про- верки	В ид П ро- верк и (пла- но- вая, вн епла- но- вая)	Ос- нова- ния про- верки	Кон- трольные мероприя- тия	ФИО, долж- ность проверя- емого лица	Резуль- таты про- верки	Номер, дата прото- кола, со- ставлен- ного по ре- зультатам проверки	Резуль- таты про- верки	ФИ О, долж- ности чле- нов ко- мис- сии	Подпись	
										Про- веряе- мого лица	Чле- нов ко- мис- сии
1	2	3	4	5	6	7	8	9	10	11	12

