УТВЕРЖДАЮ
Директор МАОУ СОШ № 7
_____ Л.Н. Вольвач
«09» 01 2018г.

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора

1. Общие положения

Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных в муниципальном автономном общеобразовательном учреждении города Калининграда средней общеобразовательной школы № 7 (далее по тексту – ОУ) требованиям к защите персональных данных разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и 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, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ОУ проводятся периодические проверки условий обработки персональных данных.

Проверка обработки персональных данных проводится комиссией, состав которой утверждается внутренним приказом.

Проверка условий обработки персональных данных проводится на основании утвержденного в ОУ ежегодного плана мероприятий по обеспечению защиты персональных данных в информационной системе персональных данных.

Результаты проведения проверок отмечаются в соответствующем журнале учета проверок с обязательным заполнением «Протокола внутренней проверки в области обработки персональных данных» (Приложение № 1).

В проведении проверки условий обработки персональных данных могут привлекаться сторонние компании-лицензиаты.

Проверка условий обработки персональных данных осуществляется непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест, участвующих в процессе обработки персональных данных.

При проведении проверки условий обработки персональных данных должны быть полностью, объективно и всесторонне установлены:

1) порядок и условия применения организационных и технических мер, необходимых для выполнения требований к защите персональных данных;

2) порядок и условия применения средств защиты информации;

3) эффективность принимаемых мер по обеспечению безопасности персональных данных до их ввода в информационные системы персональных данных;

4) состояние учета носителей персональных данных;

5) соблюдение правил доступа к персональным данным;

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

7) мероприятия по восстановлению персональных данных, модифицированных или

уничтоженных вследствие несанкционированного доступа к ним.

Комиссия по проведению проверки условий обработки персональных данных имеет право:

1) запрашивать у работников информацию, необходимую для реализации полномочий;

2) требовать от работников, осуществляющих обработку персональных данных, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

3) вносить предложения:

- о совершенствовании правового, технического и организационного обеспечения безопасности персональных данных при их обработке;

- о приостановлении или прекращении обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

- о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о персональных данных.

Члены комиссии по проведению проверки условий обработки персональных данных должны обеспечивать конфиденциальность ставших им известными в ходе проведения мероприятий внутреннего контроля персональных данных.

Приложение № 1
к правилам осуществления внутреннего
контроля соответствия обработки
персональных данных к требованиям к защите
персональных данных.

1. Организационные мероприятия

Обозначение критерия	Наименование критерия	Примечание
КО-1	Наличие действующего распоряжения о назначении ответственного лица за организацию обработки ПДн.	152-ФЗ, ст.18.1, ч.1, п.1 152-ФЗ, ст.22.1, ч.1 ПП-211, п.1-а, п.1-б
КО-2	Наличие действующего распоряжения о назначении лица, ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн (администратора безопасности ИСПДн)	ПП-1119, п.14
КО-3	Наличие действующего распоряжения о назначении постоянной комиссии по персональным данным.	Комиссия для установления уровней защищенности ПДн, для уничтожения носителей ПДн, проведения внутренних проверок и др.
КО-4	Наличие актуальных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных	152-ФЗ, ст.19, ч.2, п.1
КО-5	Наличие и ведение журнала учета машинных носителей ПДн	152-ФЗ, ст.19, ч.2, п.5
КО-6	Наличие актуального перечня мест хранения носителей ПДн	ПП-687, ч.3, п.13
КО-7	Наличие актуального перечня сотрудников, допущенных к обработке ПДн	ПП-687, ч.3, п.13 ПП-211, п.1-б
КО-8	Наличие актуального перечня ИСПДн	ПП-211, п.1-б
КО-9	Наличие актуального перечня ПДн	ПП-211, п.1-б
КО-10	Проверка наличия и актуальности внутренних организационно-распорядительных документов (Правила, положения, инструкции, регламенты, план мероприятий).	152-ФЗ, ст.18.1, ч.1, п.2 ПП-211, п.1-б
КО-11	Проверка наличия актуальных документов, определяющих политику обработки персональных данных в общедоступных источниках	152-ФЗ, ст.18.1, ч.2 ПП-211, п.2
КО-12	Проверка наличия документов, подтверждающих факт ознакомления допущенных к обработке сотрудников с	152-ФЗ, ст.18.1, ч.1, п.6 ПП-211, п.1-е

	положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, с документами, определяющими политику оператора в отношении обработки персональных данных, с локальными актами по вопросам обработки персональных данных и (или) обучения указанных сотрудников.	
КО-13	Наличие актуального (полного и достоверного) отправленного в уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор) Уведомления об обработке ПДн (письма о внесении изменений в Уведомление)	152-ФЗ, ст.22 ПП-211, п.1-ж
КО-14	Наличие согласий работников на обработку их ПДн	152-ФЗ, ст.6, ч.1, п.1 152-ФЗ, ст.9, ПП-211, п.1-б
КО-15	Наличие письменных обязательств сотрудников, допущенных к обработке ПДн, о неразглашении ПДн	ПП-211, п.1-б
КО-16	Наличие актуальных Актов установления уровней защищенности ПДн при их обработке в ИСПДн	152-ФЗ, ст.19, ч.2, п.2 ПП-1119
КО-17	Наличие соглашений (существенных условий договоров) с контрагентами о соблюдении конфиденциальности передаваемых ПДн (в случае такой передачи по договору)	152-ФЗ, ст.6, ч.3
КО-18	Наличие согласий субъектов на опубликование их ПДн в общедоступных источниках	152-ФЗ, ст.8
КО-19	Наличие и ведение журнала запросов субъектов ПДн по вопросам обработки ПДн и наличие правил обработки таких запросов	152-ФЗ, ст.14
КО-20	Проверка соблюдения оператором правил работы (хранения и уничтожения) с носителями ПДн	ПП-687
КО-21	Наличие актуального плана мероприятий по обеспечению безопасности ПДн и ведение журнала внутренних проверок в области обработки ПДн	152-ФЗ, ст.18.1, ч.1, п.4 ПП-211, п.1-б, п.1-д
КО-22	Проверка соблюдения сотрудниками правил доступа в помещения, в которых происходит обработка и хранение бумажных носителей ПДн, а также в которых	ПП-1119, п. 13-а ПП-211, п.1-б

	расположены компоненты ИСДПн	
КО-23	Выявление избыточных данных по отношению к целям обработки	152-ФЗ, ст.5, ч.5
КО-24	Своевременность проведения мероприятий по обезличиванию персональных данных	152-ФЗ, ст.5, ч.7 ПП-211, п.1-б, п.1-з
КО-25	Своевременность проведения мероприятий по уничтожению персональных данных	152-ФЗ, ст.5, ч.7

2. Технические мероприятия

Обозначение критерия	Наименование критерия
КТ-1	Соблюдение порядка разграничения прав доступа к ИСПДн
КТ-2	Применение антивирусной защиты в ИСПДн
КТ-3	Применение средств резервного копирования и восстановления в ИСПДн
КТ-4	Применение надежных паролей для доступа к ИСПДн
КТ-5	Применение шифровальных средств для защиты информации при передаче ПДн по каналам связи за пределы контролируемой зоны
КТ-6	Применение сертифицированных средств защиты в ИСПДн
КТ-7	Расположение технических средств ИСПДн в пределах контролируемой зоны, исключающее случайный или преднамеренный несанкционированный просмотр выводимых данных
КТ-8	Соблюдение пользователями правил работы со съемными машинными носителями ПДн
КТ-9	Соблюдение пользователями правил работы с шифровальными средствами
КТ-10	Соблюдение пользователями правил работы с СЗИ в ИСПДн
КТ-11	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей
КТ-12	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
КТ-13	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации
КТ-14	Контроль состава технических средств, программного обеспечения и средств защиты информации