*Общеобразовательная автономная некоммерческая организация*
*«Классическая Православная гимназия святого праведного Иоанна Кронштадтского»*
*143988 Московская область, г.о. Балашиха, мкр. Павлино, д. 13*
*e-mail: melnichuk-52@mail.ru, тел. (495) 527-48-40 сайт: www.klass-gim.ru*
***ОКПО 81719687, ОГРН 1165000053866, ИНН/КПП 5012092703/501201001***

УТВЕРЖДАЮ
Директор ОАНО КПГСПИК
В.М. Мельничук
«05» июня 20 20 г.

**ПРАВИЛА осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ОАНО КПГСПИК**

## 1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее — Правила) в ОАНО КПГСПИК (далее — Учреждении), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее — ПД); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПД, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПД.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «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», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211.

1.3. Пользователем (далее — Пользователь) является сотрудник Учреждения участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПД и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее — СЗИ) ПД.

1.4. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных Учреждения проводятся в следующих целях:

1.4.1. проверка выполнения требований организационно-распорядительной документации по защите информации в Учреждении и действующего

законодательства Российской Федерации в области обработки и защиты персональных данных;

1.4.2 оценка уровня осведомленности и знаний работников Учреждения в области обработки и защиты персональных данных;

1.4.3 оценка обоснованности и эффективности применяемых мер и средств защиты.

## 2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПД требованиям к защите ПД:

2.1. Проверки соответствия обработки ПД установленным требованиям в Учреждении разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся директором периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее — План, приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в Учреждении.

2.3. 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 в Учреждении.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3 по решению директора Учреждения.

## 3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

## 4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности.

4.2.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.2.1 описание проведенных мероприятий по каждому из этапов;

4.2.2 перечень и описание выявленных нарушений;

4.2.3 рекомендации по устранению выявленных нарушений;

4.2.4 заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. Общая информация о проведенных контрольных мероприятиях фиксируется в Журнале учета событий информационной безопасности.

4.4. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении (приложение 2).

## 5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПД в Учреждении.

5.2. Лицо, ответственное за обеспечение безопасности ПД, не позднее, чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех работающих с ПД, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

- Соответствие полномочий Пользователя правилам доступа.
- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПД.
- Соблюдение инструкций и регламентов по обеспечению безопасности информации в Учреждении.

- Соблюдение Порядка доступа в помещения Учреждения, где ведется обработка персональных данных.
- Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПД при возникновении внештатных ситуаций.
- Знание инструкций и регламентов по обеспечению безопасности информации в Учреждении.
- Порядок и условия применения средств защиты информации.
- Состояние учета машинных носителей персональных данных.
- Наличие (отсутствие) фактов несанкционированного доступа к ПД и принятие необходимых мер.
- Проведенные мероприятия по восстановлению ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Технические мероприятия, связанные с штатным и нештатным функционированием средств защиты.
- Технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации.

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**
**ОАНО КПГСПИК**

| **Тема проверки** | **Предполагаемая дата** | **Исполнитель** |
|---|---|---|
| Соблюдение парольной и антивирусной политики, использование средств защиты информации | Апрель | Ответственный за организацию работы по обработке персональных данных |
| Соблюдение порядка доступа в помещения, в которых ведется обработка персональных данных | Август | Ответственный за организацию работы по обработке персональных данных |

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 ОАНО КПГСПИК

Настоящий Протокол составлен в том, что «____»_____202__г.
Комиссией в составе

_____
(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:
Члены комиссии: