**Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение**
**«ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ ГОРОДСКОГО ХОЗЯЙСТВА»**
(СПб ГБПОУ «ПКГХ»)

# ПРИКАЗ

30 декабря 2022 года № 1085-ОД

**Об утверждении нормативного локального акта и Комиссии по классификации информационных систем персональных данных**

Во исполнение статьи 16 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»

**П Р И К А З Ы В А Ю:**

1. Утвердить прилагемый Регламент проведения классификации информационных систем персональных данных (Приложение №1).
2. Сформировать комиссию по классификации информационных систем персональных данных Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Политехнический колледж городского хозяйства» по требованиям защиты информации (далее – Комиссия) в составе согласно Приложению №2.
3. Комиссии в срок до 15.01.2023 провести определение класса защищенности информационных систем персональных данных в соответствии с Приказом Федеральной службы по техническому и экспортному контролю России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и уровня защищенности персональных данных, обрабатываемых в информационных системах в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Регламентом проведения классификации информационных систем персональных данных с учетом актуальных угроз безопасности, определенных Моделью угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных.
4. Контроль за выполнением настоящего приказа оставляю за собой.

Директор В.М.Малиновский

Исполнитель:
Начальник отдела ИО и ПП
Ваганов С.В.

Приложение №1

УТВЕРЖДЕН
приказом директора
от 30.12 2022
№ 1085 - ОД

# РЕГЛАМЕНТ
## проведения классификации информационных систем персональных данных

### 1. Термины и сокращения

**Персональные данные (ПДн)** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Оператор** — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**Обработка персональных данных** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Автоматизированная обработка персональных данных** — обработка персональных данных с помощью средств вычислительной техники.

**Распространение персональных данных** — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

**Предоставление персональных данных** — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

**Блокирование персональных данных** — временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Уничтожение персональных данных** — действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

**Обезличивание персональных данных** — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Информационная система персональных данных (ИСПДн)** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Трансграничная передача персональных данных** — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**Типовая информационная система** — информационная система, в которой требуется обеспечение только конфиденциальности персональных данных.

**Специальная информационная система** — информационная система, в которой вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

## 2. Общие положения

2.1. Настоящий Регламент определяет обязательный порядок проведения классификации информационных систем персональных данных.

Проведение классификации информационных систем персональных данных возлагается на Комиссию по приведению в соответствие с требованиями законодательства в области персональных данных.

## 3. Методика проведения классификации ИСПДн

3.1. Классификация ИСПДн включает в себя следующие этапы:

3.1.1. Анализ исходных данных об ИСПДн.

3.1.2. Оценка степени возможных последствий для субъекта ПДн в случае нарушения характеристик безопасности ПДн.

3.1.3. Присвоение класса ИСПДн и документальное оформление результатов классификации.

### 3.2.Анализ исходных данных об ИСПДн

3.2.1. Анализ исходных данных об ИСПДн проводится на основании Перечня информационных систем персональных данных, в котором содержится информация об основных классификационных характеристиках ИСПДн в соответствии с Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»:

категория обрабатываемых персональных данных (Хпд);

- объем обрабатываемых персональных данных (Хнпд);
- требуемые характеристики безопасности персональных данных – конфиденциальность, целостность, доступность;
- структура информационной системы;

- наличие подключения к сетям связи общего пользования и/или сетям международного информационного обмена;
- режим обработки персональных данных;
- наличие разграничения доступа;
- местонахождение технических средств информационной системы. На основании сведений и в соответствии с Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» определяется тип ИСПДн, типовая или специальная, и предварительный класс ИСПДн.

**3.3. Оценка степени возможных последствий для субъекта пдн в случае нарушения характеристик безопасности ПДн**

Второй этап проводится в том случае, если были выявлены специальные ИСПДн и только для них.

На данном этапе определяется степень возможных последствий для субъекта ПДн при нарушении характеристик безопасности ПДн (реализации угроз) при автоматизированной обработке ПДн в ИСПДн.

Так же на данном этапе определяются вербальные показатели опасности угроз в ИСПДн. Угрозы имеют три значения:

- низкая опасность — реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;
- средняя опасность — реализация угрозы может привести к негативным последствиям для субъектов ПДн;
- высокая опасность — реализация угрозы может привести к значительным негативным последствиям для субъектов ПДн.

Степень возможных последствий для субъекта ПДн проводится на основании экспертной оценки специалистов по информационной безопасности в соответствии с документом «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. Заместителем директора ФСТЭК России 14.02.2008).

В качестве данных для анализа Комиссией рассматриваются следующие документы:

- Перечень должностей и третьих лиц, имеющих доступ к персональным данным;
- Перечень персональных обрабатываемых данных;
- Перечень информационных систем персональных данных;
- Технический паспорт информационных систем персональных данных;
- Перечень применяемых средств защиты информации.

Анализ степени возможных последствий для субъекта ПДн проводится для каждой из характеристик безопасности информации в отдельности:

- нарушение конфиденциальности ПДн (копирование, неправомерное распространение) – неконтролируемое распространение ПДн или получение

доступа к ПДн без согласия субъекта ПДн или наличия иного законного основания лицами, не допущенными к обработке ПДн;
- нарушение целостности ПДн (уничтожение, изменение) – преднамеренное или непреднамеренное изменение ПДн;
нарушение доступности ПДн (блокирование) – временная невозможность осуществлять сбор, систематизацию, накопление, использование, распространение или передачу персональных данных. Поскольку показатель опасности угрозы является вербальным, то необходимо ввести четкие критерии для определения степени последствий для субъекта ПДн и соответственно показателя опасности угрозы. В Таблице 1 приведены базовые критерии, которые могут быть использованы для проведения классификации. В отдельных случаях Комиссией может быть принято решение о выборе иных критериев.

**Таблица №1**

**Критерии**
**оценки последствий для субъекта ПДн и соответствующие им показатели опасности угроз**

| Критерий оценки последствий для субъекта ПДн | Степень последствий для субъекта ПДн | Показатель опасности угрозы |
|---|---|---|
| При нарушении характеристик безопасности ПДн:<br>последствия для субъекта ПДн незаметны либо мало ощутимы;<br>отсутствует измеримый финансовый, репутационный, моральный ущерб для субъекта ПДн;<br>репутация субъекта ПДн, его материальное благополучие, жизнь и здоровье не затронуты;<br>основные интересы и права субъекта ПДн, закрепленные Конституцией РФ, не затронуты. | Незначительные негативные последствия | Низкая опасность |
| При нарушении характеристик безопасности ПДн:<br>последствия для субъекта ПДн приводят к измеримым, но малым по объему или значению финансовым и/или моральным и/или репутационным потерям;<br>жизнь и здоровье субъекта ПДн не затронуты;<br>основные интересы и права | Негативные последствия | Средняя опасность |

| | | |
|---|---|---|
| субъекта ПДн, закрепленные Конституцией РФ, не затронуты. | | |
| При нарушении характеристик безопасности ПДн:<br>последствия для субъекта ПДн приводят к ощутимым финансовым, моральным, репутационным потерям, вплоть до потери средств к существованию;<br>возможно влияние на состояние здоровье или угрозы для жизни субъекта ПДн. | Значительные негативные последствия | Высокая опасность |

После выбора критериев оценки последствий для субъекта ПДн Комиссия определяет показатели опасности нарушения конфиденциальности, целостности и доступности.

Исходя из определенных показателей опасности угроз, Комиссией устанавливаются итоговые максимальные значения показателей опасности угроз для каждой характеристики безопасности.

**3.3. Присвоение класса испдн и документальное оформление результатов классификации**

3.3.1. Класс ИСПДн определяется исходя из максимального показателя опасности угроз, установленных для каждой характеристики безопасности:

**- класс К1** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;

**- класс К2** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

**- класс К3** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

**- класс К4** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных. Результаты классификации каждой ИСПДн оформляются документом «Акт классификации ИСПДн». Форма Акта классификации приведена в Приложении № 2 к настоящему Регламенту.

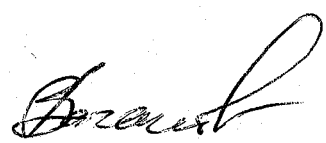
## 4. Пересмотр класса ИСПДн

4.1. Класс ИСПДн может быть пересмотрен:

- по решению Комиссии на основании проведенного анализа и оценки угроз безопасности персональных данных с учетом особенностей и/или изменений конкретной информационной системы;
- по результатам внутренних и внешних мероприятий по контролю за выполнением требований по обеспечению безопасности персональных данных при их обработке в ИСПДн. Изменения особенностей ИСПДн, следствием которых может стать пересмотр ее класса, включают: □ изменение категории персональных данных, обрабатываемых в ИСПДн;
- изменения целей обработки персональных, следствием которых может стать изменение степени возможных последствий для субъекта ПДн при нарушении характеристик безопасности ПДн. Комиссия ведет План по пересмотру класса ИСПДн, который представлен в Приложении 3 к настоящему Регламенту. Результаты работы Комиссии по определению нового класса ИСПДн оформляется в виде Протокола определения ущерба и Акта классификации информационных систем персональных данных.

## 5. Пересмотр и внесение изменений

5.1. Пересмотр положений настоящего документа и внесение изменений производятся в случаях, указанных в Регламенте по реагированию на инциденты информационной безопасности.

Разработчик
Начальник отдела ИО и ПП  С.В.Ваганов