Приложение № 4
к Приказу № 30-од
от 12 марта 2020 г.

РЕГЛАМЕНТ
ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Литературный институт имени А.М. Горького»

г. МОСКВА, 2020 г.

СОДЕРЖАНИЕ

1. Термины и сокращения 3
2. Общие положения 3
3. Методика определения уровня защищенности ПДн, обрабатываемых в ИСПДн 4
   3.1. Определение уровня защищенности ИСПДн включает в себя следующие этапы: 4
   3.2. Анализ исходных данных об ИСПДн 4
   3.3. Оценка степени возможных последствий для субъекта ПДн в случае нарушения характеристик безопасности ПДн и определение типа угроз, актуальных для ИСПДн 4
   3.4. Присвоение уровня защищенности ПДн, обрабатываемых в ИСПДн, и документальное оформление результатов 7
4. Пересмотр уровня защищенности ПДн, обрабатываемых ИСПДн 8
5. Пересмотр и внесение изменений 9
Приложение №1 10
Приложение №2 14
Приложение №3 15

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.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Регламент определяет порядок определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных в ФГБОУ ВО «Литературный институт имени А.М. Горького».

2.2. Определение уровня защищенности ПДн, обрабатываемых в ИСПДн, в ФГБОУ ВО «Литературный институт имени А.М. Горького» возлагается на Комиссию

по приведению ФГБОУ ВО «Литературный институт имени А.М. Горького» в соответствие с требованиями законодательства в области ПДн.

2.3. Контроль за исполнением положений настоящего Регламента возлагается на ответственного за организацию обработки персональных данных.

3. МЕТОДИКА ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПДН, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Определение уровня защищенности ИСПДн включает в себя следующие этапы:

- анализ исходных данных об ИСПДн;
- оценка степени возможных последствий для субъекта ПДн в случае нарушения характеристик безопасности ПДн и определение типа угроз, актуальных для ИСПДн;
- присвоение уровня защищенности ПДн, обрабатываемых в ИСПДн;
- документальное оформление результатов.

3.2. Анализ исходных данных об ИСПДн

Анализ исходных данных об ИСПДн проводится на основании Модели угроз и нарушителя безопасности информации ИСПДн и Перечня ИСПДн, в котором содержится информация об основных характеристиках ИСПДн:

- состав обрабатываемых ПДн;
- объем обрабатываемых ПДн;
- характеристики безопасности ПДн;
- структура ИСПДн;
- наличие подключения к сетям международного обмена;
- режим обработки ПДн;
- разграничение прав доступа;
- местонахождение ИСПДн;
- работники, имеющие доступ к ПДн.

3.2.1. На основании указанных сведений и в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» будет определен уровень защищенности персональных данных, обрабатываемых в ИСПДн.

3.3. Оценка степени возможных последствий для субъекта ПДн в случае нарушения характеристик безопасности ПДн и определение типа угроз, актуальных для ИСПДн

3.3.1. Второй этап производится оператором во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных». На данном этапе определяется степень возможных последствий для субъекта ПДн при нарушении характеристик безопасности ПДн (реализации угроз) при автоматизированной обработке ПДн в ИСПДн.

3.3.2. 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.

3.3.3. Степень возможных последствий для субъекта ПДн проводится на основании экспертной оценки Комиссии, 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).

3.3.4. В качестве данных для анализа Комиссией рассматриваются следующие документы:

- Перечень должностей и третьих лиц, имеющих доступ к ПДн;
- Перечень ПДн;
- Перечень ИСПДн;
- Технический паспорт ИСПДн.
- Перечень применяемых средств защиты информации.

3.3.5. 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.

3.3.6. 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 определения уровней защищенности ПДн, при их обработке в ИСПДн. 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: - последствия для субъекта ПДн незаметны либо малоощутимы; - отсутствует измеримый финансовый, репутационный, моральный ущерб для субъекта ПДн; - репутация субъекта ПДн, его материальное благополучие, жизнь и здоровье не затронуты; - основные интересы и права субъекта ПДн, закрепленные Конституцией РФ, не затронуты.	Незначительные негативные последствия	Низкая опасность
При нарушении характеристик безопасности ПДн: - последствия для субъекта ПДн приводят к измеримым, но малым по объему или значению финансовым и/или моральным и/или репутационным потерям; - жизнь и здоровье субъекта ПДн не затронуты; - основные интересы и права субъекта ПДн, закрепленные Конституцией РФ, не затронуты.	Негативные последствия	Средняя опасность
При нарушении характеристик безопасности ПДн: - последствия для субъекта ПДн приводят к ощутимым финансовым, моральным, репутационным потерям, вплоть до потери средств к существованию; - возможно влияние на состояние здоровье или угрозы для жизни субъекта ПДн.	Значительные негативные последствия	Высокая опасность

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

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

3.3.9. На основании полученных итоговых максимальных значений показателей опасности угроз определяется тип угроз, актуальных для ИСПДн:

- Высокая опасность - Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе

- Средняя опасность - Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе

- Низкая опасность - Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных

(недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе

3.3.10. Результаты работы Комиссии по оценке степени возможных последствий для субъекта ПДн оформляются в виде Протокола заседания Комиссии по определению показателя угроз безопасности ПДн при их обработке в ИСПДн, приведенного в Приложении №1 к настоящему Регламенту.

3.4. Присвоение уровня защищенности ПДн, обрабатываемых в ИСПДн, и документальное оформление результатов

3.4.1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, определяется исходя из типа угроз, актуального для ИСПДн, состава и объема обрабатываемых ПДн.

3.4.2. Необходимость обеспечения 1-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа, и информационная система обрабатывает либо специальные категории ПДн, либо биометрические персональные данные, либо иные категории ПДн;
- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора.

3.4.3. Необходимость обеспечения 2-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 1-го типа, и информационная система обрабатывает общедоступные ПДн;
- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает специальные категории ПДн работников оператора или специальные категории персональных данных менее чем 100000 субъектов ПДн, не являющихся работниками оператора;
- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает биометрические ПДн;
- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает общедоступные ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора;
- для информационной системы актуальны угрозы 2-го типа, и информационная

система обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора.

3.4.4. Необходимость обеспечения 3-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 2-го типа, и информационная

система обрабатывает общедоступные ПДн работников оператора или общедоступные ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 2-го типа, и информационная система обрабатывает иные категории ПДн работников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает специальные категории ПДн работников оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора;

- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает биометрические ПДн;

- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся работниками оператора.

3.4.5. Необходимость обеспечения 4-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает общедоступные ПДн;

- для информационной системы актуальны угрозы 3-го типа, и информационная система обрабатывает иные категории ПДн работников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся работниками оператора.

3.4.6. Результаты определения уровня защищенности ПДн для каждой ИСПДн оформляются документом «Акт определения уровня защищенности ПДн, обрабатываемых ИСПДн». Форма Акта приведена в Приложении №2 к настоящему Регламенту.

4. ПЕРЕСМОТР УРОВНЯ ЗАЩИЩЕННОСТИ ПДН, ОБРАБАТЫВАЕМЫХ ИСПДн

4.1. Уровень защищенности ПДн, обрабатываемых в ИСПДн, может быть пересмотрен:

- по решению Комиссии на основании проведенного анализа и оценки угроз безопасности ПДн с учетом особенностей и/или изменений конкретной информационной системы;

- по результатам внутренних и внешних мероприятий по контролю за выполнением требований по обеспечению безопасности ПДн при их обработке в ИСПДн.

4.2. Изменения особенностей ИСПДн, следствием которых может стать пересмотр уровня защищенности обрабатываемых в ней ПДн, включают:

- изменение категории ПДн, обрабатываемых в ИСПДн;

- изменения целей обработки ПДн, следствием которых может стать изменение степени возможных последствий для субъекта ПДн при нарушении характеристик безопасности ПДн.

4.3. Комиссия ведет План по пересмотру уровня защищенности ПДн, обрабатываемых в ИСПДн, который представлен в Приложении №3 к настоящему Регламенту. Результаты работы Комиссии по определению нового уровня защищенности

оформляется в виде Протокола заседания комиссии по определению показателя угроз безопасности ПДн при их обработке в ИСПДн и Акта определения уровня защищенности ПДн, обрабатываемых в ИСПДн.

4.4. Пересмотр уровня защищенности ПДн, обрабатываемых в ИСПДн, производится не реже, чем 1 раз в год.

5. ПЕРЕСМОТР И ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Пересмотр положений настоящего документа и внесение изменений производятся в случаях, указанных в организационно-распорядительных документах по защите информации в Министерстве культуры Российской Федерации.

ПРИЛОЖЕНИЕ №1

Типовая форма

ПРОТОКОЛ №_____
ЗАСЕДАНИЯ КОМИССИИ ПО ПРИВЕДЕНИЮ В СООТВЕТСТВИЕ
ФГБОУ ВО «Литературный институт имени А.М. Горького»
С ТРЕБОВАНИЯМИ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ

г. Москва «__»_____20___ г.

Цель заседания Комиссии: определение показателя опасности угроз безопасности персональных данных при их обработке в информационной системе персональных данных «_____» и, как следствие, определение типа угроз, актуальных в информационной системе персональных данных «_____».

Комиссия по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных:

_____ _____ _____

Состав комиссии:

_____ _____ _____
_____ _____ _____
_____ _____ _____

Повестка заседания:

Определить степень возможных последствий для субъекта персональных данных при нарушении характеристик безопасности данных (реализации угроз) при автоматизированной обработке данных в информационной системе персональных данных «_____» и, как следствие, определить вербальный показатель опасности угроз в информационной системе персональных данных «_____», который может иметь три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Исходные данные по информационной системе персональных данных «_____» и обрабатываемым в них персональным данным приведены в Перечне обрабатываемых персональных данных, Перечне информационных систем персональных данных и Техническом паспорте информационных систем персональных данных.

Оценка степени возможных последствий для субъекта ПДн производится в соответствии со следующими документами:

«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 исходных данных рассматриваются следующие документы:

- Перечень персональных данных;
- Перечень информационных систем персональных данных;
- Технический паспорт ИСПДн.

Перечень ПДн используется для анализа целей обработки ПДн и, соответственно, возможных последствий для субъекта ПДн в случае нарушения целостности или доступности ПДн, повлекших за собой невозможность достижения указанных целей. Перечень и описания ИСПДн необходимы для анализа состава и объема обрабатываемых ПДн в конкретной ИСПДн, анализа целей обработки ПДн и, соответственно, возможных последствий для субъекта ПДн в случае нарушения конфиденциальности, целостности или доступности ПДн.

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 конфиденциальности не влияет на функционирование процессов обработки ПДн;

- нарушение целостности ПДн (уничтожение, изменение) - преднамеренное или непреднамеренное изменение ПДн. Нарушение целостности ПДн не влияет на возможность функционирования процессов обработки ПДн, но приводит к тому, что в рамках процесса могут быть приняты неверные решения в отношении субъекта ПДн. Соответственно, для определения степени возможных последствий для субъекта ПДн при нарушении целостности ПДн необходимо проанализировать возможные последствия в каждом отдельном процессе и в отношении определенных баз данных. Кроме того, нарушение целостности может приводить в том числе к нарушению доступности ПДн;

- нарушение доступности ПДн (блокирование) - временная невозможность осуществлять сбор, систематизацию, накопление, использование, распространение или передачу персональных данных. Нарушение доступности ПДн влияет на возможность функционирования процессов обработки ПДн и, как следствие, на достижение целей обработки ПДн в рамках этих процессов. Соответственно, для определения степени возможных последствий для субъекта ПДн при нарушении доступности ПДн необходимо проанализировать возможные последствия в каждом отдельном процессе и в отношении определенных баз данных.

Принятые решения:

1. Комиссией были приняты следующие критерии для определения степени последствий для субъекта ПДн и соответственно показателя опасности угрозы (Таблица 1):

Таблица 1. Критерии определения последствий для субъекта персональных данных и соответствующие им показатели опасности угроз.

Критерий оценки последствий для субъекта персональных данных	Степень последствий для субъекта персональных данных	Показатель опасности угрозы
При нарушении характеристик безопасности персональных данных: - последствия для субъекта персональных данных незаметны либо мало ощутимы; - отсутствует измеримый финансовый, репутационный, моральный ущерб для субъекта персональных данных; - репутация субъекта персональных данных, его материальное благополучие, жизнь и здоровье не затронуты; - основные интересы и права субъекта персональных данных, закрепленные Конституцией РФ, не затронуты.	Незначительные негативные последствия	Низкая опасность
При нарушении характеристик безопасности персональных данных: - последствия для субъекта персональных данных приводят к измеримым, но малым по объему или значению финансовым и/или моральным и/или репутационным потерям; - жизнь и здоровье субъекта персональных данных не затронуты; - основные интересы и права субъекта персональных данных, закрепленные Конституцией РФ, не затронуты.	Негативные последствия	Средняя опасность
При нарушении характеристик безопасности персональных данных: - последствия для субъекта персональных данных	Значительные негативные последствия	Высокая опасность
приводят к ощутимым финансовым, моральным, репутационным потерям, вплоть до потери средств к существованию; - возможно влияние на состояние здоровье или угрозы для жизни субъекта персональных данных.		

2. Для каждой группы персональных данных, обрабатываемых в информационной системе персональных данных «_____», исходя из критериев, принятых в Таблице 1, установить следующие показатели опасности нарушения конфиденциальности персональных данных (Таблица 2):

Таблица 2. Показатели опасности нарушения конфиденциальности для каждой группы персональных данных

/п	Группа персональных данных	Степень последствий для субъекта персональных данных	Показатель опасности угрозы
	Персональные данные _____	Негативные последствия	Средняя опасность

3. Для каждого процесса обработки ПДн, входящего в ИСПДн «_____» исходя из критериев, принятых в п. 1, установить следующие показатели опасности нарушения целостности ПДн (Таблица 3):

Таблица 3. Показатели опасности нарушения целостности персональных данных

/п	Группа персональных данных	Степень последствий для субъекта персональных данных	Показатель опасности угрозы
	Персональные данные _____	Негативные последствия	Средняя опасность

4. Для каждого процесса обработки ПДн, входящего в ИСПДн «_____», исходя из критериев, принятых в п. 1, установить следующие показатели опасности нарушения доступности ПДн (Таблица 4):

Таблица 4. Показатели опасности нарушения доступности персональных данных

п	Группа персональных данных	Степень последствий для субъекта персональных данных	Показатель опасности угрозы
	Персональные данные ___	Негативные последствия	Средняя опасность

5. Исходя из показателей опасности угроз, определенных в пунктах 2, 3 и 4, установить для «_____» следующие наивысшие значения показателей опасности угроз для каждой характеристики безопасности:

- нарушение конфиденциальности - опасность;
- нарушение целостности - опасность;
- нарушение доступности - опасность.

ПРИЛОЖЕНИЕ №2

Типовая форма

АКТ №1
определения уровня защищенности персональных данных, обрабатываемых в информационной системе персональных данных «_____» от «___»_____20____ г.

Комиссия по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных:

_____ _____ _____

Состав комиссии:

_____ _____ _____
_____ _____ _____
_____ _____ _____

рассмотрела исходные данные информационной системы персональных данных «_____»:

Категория обрабатываемых персональных данных (Хпд)	Хпд = _____. Обрабатываются обезличенные и (или) общедоступные персональные данные.
Объем обрабатываемых персональных данных (Хнпд)	Хнпд = _____. В информационной системе одновременно обрабатываются данные менее чем _____ субъектов персональных данных.
Требуемые характеристики безопасности персональных данных	Информационная система персональных данных, для которой необходимо обеспечить защиту персональных данных от нарушения следующих характеристик безопасности _____.
Структура информационной системы	_____
Подключение информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена	_____
Режим обработки персональных данных	_____
Разграничение доступа	_____
Местонахождение технических средств информационной системы	_____

Согласно Протоколу №_____ заседания Комиссии по определению показателя угроз безопасности персональных данных при их обработке в информационных системах персональных данных в ФГБОУ ВО «Литературный институт имени А.М. Горького», для информационной системы персональных данных «_____» актуальны **Угрозы -го типа.**

В соответствии с Регламентом определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных, Протоколом заседания Комиссии по определению показателя угроз безопасности персональных данных при их обработке в информационных системах персональных данных, Постановлением Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также в результате анализа исходных данных и проведенного анализа и оценки угроз безопасности персональных данных с учетом особенностей данной информационной системы,

РЕШИЛА:

1. Установить персональным данным, обрабатываемым в информационной системе персональных данных «_____»,_____-й уровень защищенности.

ПРИЛОЖЕНИЕ №3

Типовая форма

ПЛАН
пересмотра уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных

п/п	Дата	Названия ИСПДн	Новый УЗ	Основание пересмотра	Подписи комиссии
				Плановый пересмотр	**Комиссия по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных:** _____
				Плановый пересмотр	
				Плановый пересмотр	
				Плановый пересмотр	