МИНИСТЕРСТВО КУЛЬТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
ЕКАТЕРИНБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ТЕАТРАЛЬНЫЙ ИНСТИТУТ

ПРИКАЗ

от 03.04.2020 № 49-общ

г. Екатеринбург

Об утверждении локальных нормативных актов об обработке персональных данных и обеспечении их безопасности

В соответствии с Федеральным законом Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 21.03.2012 №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 Постановлением Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»:

ПРИКАЗЫВАЮ:

1. Утвердить локальные нормативные акты об обработке персональных данных и обеспечении их безопасности:
– Политика федерального государственного бюджетного образовательного учреждения высшего образования «Екатеринбургский государственный театральный институт» (Приложение 1);
– Положение об обработке персональных данных (Приложение 2);
– Положение об обеспечении безопасности персональных данных (Приложение 3);
– Регламент определения уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных федерального государственного бюджетного образовательного учреждения высшего образования «Екатеринбургский государственный театральный институт» (Приложение 4).
2. Оперативно довести до сведения ответственных работников данный приказ под роспись и обеспечить хранение листов ознакомления работников в подразделениях.

3. Специалисту по связям с общественностью Немченко Е.Ю. обеспечить незамедлительное размещение настоящего приказа на официальном сайте Екатеринбургского государственного театрального института.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Ректор А.А. Глуханюк

Приложение № 1
к Приказу №49-ОД от «03» апреля 2020 г

ПОЛИТИКА
федерального государственного бюджетного образовательного учреждения высшего образования «Екатеринбургский государственный театральный институт»

в отношении обработки персональных данных

г. Екатеринбург, 2020 г.

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Политика обработки персональных данных (далее - Политика) разработана в соответствии с Федеральным законом от 27.07.2006. №152-ФЗ «О персональных данных» (далее - ФЗ-152).

Настоящая Политика определяет порядок обработки персональных данных и меры по обеспечению безопасности персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Екатеринбургский государственный театральный институт» (далее - Оператор) с целью защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В Политике используются следующие основные понятия:

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных, и обеспечивающих их обработку информационных технологий и технических средств;

обезличивание персональных данных - действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных;

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;

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;

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;

уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) результате которых уничтожаются материальные носители персональных данных.

Федеральное государственное бюджетное образовательное учреждение высшего

образования «Екатеринбургский государственный театральный институт» обязан опубликовать или иным образом обеспечить неограниченный доступ к настоящей Политике обработки персональных данных в соответствии с ч. 2 ст. 18.1. ФЗ-152.

2 ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Принципы обработки персональных данных

Обработка персональных данных у Оператора осуществляется на основе следующих принципов:

- законности и справедливой основы;
- ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;
- недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;
- недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработки только тех персональных данных, которые отвечают целям их обработки;
- соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;
- недопущения обработки персональных данных, избыточных по отношению к заявленным целям их обработки;
- обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;
- уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Оператором допущенных нарушений персональных данных, если иное не предусмотрено федеральным законом.

2.2 Условия обработки персональных данных

Оператор производит обработку персональных данных при наличии хотя бы одного из следующих условий:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;
- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
- обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - общедоступные персональные данные);

- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

2.3 Конфиденциальность персональных данных

Оператор и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.4 Общедоступные источники персональных данных

В целях информационного обеспечения у Оператора могут создаваться общедоступные источники персональных данных субъектов персональных данных, в том числе справочники и адресные книги. В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, дата и место рождения, должность, номера контактных телефонов, адрес электронной почты и иные персональные данные, сообщаемые субъектом персональных данных.

Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных, уполномоченного органа по защите прав субъектов персональных данных либо по решению суда.

2.5 Специальные категории персональных данных

Обработка Оператором специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, допускается в случаях, если:

- субъект персональных данных дал согласие в письменной форме на обработку своих персональных данных;

- персональные данные сделаны общедоступными субъектом персональных данных;

- обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно;

- обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

- обработка персональных данных необходима для установления или осуществления прав субъекта персональных данных или третьих лиц, а равно и в связи с осуществлением правосудия;

- обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

Обработка специальных категорий персональных данных, осуществлявшаяся в

случаях, предусмотренных пунктом 4 статьи 10 ФЗ-152 должна быть незамедлительно прекращена, если устранены причины, вследствие которых осуществлялась их обработка, если иное не установлено федеральным законом.

Обработка персональных данных о судимости может осуществляться Оператором исключительно в случаях и в порядке, которые определяются в соответствии с федеральными законами.

2.6 Биометрические персональные данные

Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность - биометрические персональные данные - могут обрабатываться Оператором только при наличии согласия субъекта персональных данных в письменной форме.

2.7 Поручение обработки персональных данных другому лицу

Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора. Лицо, осуществляющее обработку персональных данных по поручению Оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные ФЗ-152 и настоящей Политикой.

2.8. Обработка персональных данных граждан Российской Федерации

В соответствии со статьей 2 Федерального закона от 21 июля 2014 года №242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев:

- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве (далее - исполнение судебного акта);
- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года №210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;
- обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных.

2.9. Трансграничная передача персональных данных

Оператор обязан убедиться в том, что иностранным государством, на территорию которого предполагается осуществлять передачу персональных данных, обеспечивается адекватная защита прав субъектов персональных данных, до начала осуществления такой передачи.

Трансграничная передача персональных данных на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов персональных данных, может осуществляться в случаях:

- наличия согласия в письменной форме субъекта персональных данных на трансграничную передачу его персональных данных;
- исполнения договора, стороной которого является субъект персональных данных.

3. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Согласие субъекта персональных данных на обработку его персональных данных

Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом.

3.2. Права субъекта персональных данных

Субъект персональных данных имеет право на получение у Оператора информации, касающейся обработки его персональных данных, если такое право не ограничено в соответствии с федеральными законами. Субъект персональных данных вправе требовать от Оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с субъектом персональных данных (потенциальным потребителем) с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных.

Оператор обязан немедленно прекратить по требованию субъекта персональных данных обработку его персональных данных в вышеуказанных целях.

Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных федеральными законами, или при наличии согласия в письменной форме субъекта персональных данных.

Если субъект персональных данных считает, что Оператор осуществляет обработку его персональных данных с нарушением требований ФЗ-152 или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Оператора в Уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда.

4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Безопасность персональных данных, обрабатываемых Оператором, обеспечивается реализацией правовых, организационных и технических мер, необходимых для обеспечения требований федерального законодательства в области защиты персональных данных.

Для предотвращения несанкционированного доступа к персональным данным Оператором применяются следующие организационно-технические меры:

- назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;
- ограничение состава лиц, допущенных к обработке персональных данных;
- ознакомление субъектов с требованиями федерального законодательства и нормативных документов Оператора по обработке и защите персональных данных;
- организация учета, хранения и обращения носителей, содержащих информацию с персональными данными;
- определение угроз безопасности персональных данных при их обработке, формирование на их основе моделей угроз;
- разработка на основе модели угроз системы защиты персональных данных;
- проверка готовности и эффективности использования средств защиты информации;
- разграничение доступа пользователей к информационным ресурсам и программно-аппаратным средствам обработки информации;
- регистрация и учет действий пользователей информационных систем персональных данных;
- использование антивирусных средств и средств восстановления системы защиты персональных данных;
- применение (в случае необходимости) средств межсетевого экранирования, обнаружения вторжений, анализа защищенности и средств криптографической защиты информации;
- организация пропускного режима на территорию Оператора, охраны помещений с техническими средствами обработки персональных данных.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Иные права и обязанности Оператора в связи с обработкой персональных данных определяются законодательством Российской Федерации в области персональных данных.

Работники Оператора, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Приложение № 2
к Приказу № 49-ОБУ от « 03 » апреля 2020 г.

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
федерального государственного бюджетного образовательного учреждения высшего образования «Екатеринбургский государственный театральный институт»

г. Екатеринбург, 2020 г.

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Положение об обработке персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Екатеринбургский государственный театральный институт» (далее – Положение) разработано в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - ФЗ-152), Трудовым кодексом Российской Федерации (далее - ТК РФ), а также «Перечнем сведений конфиденциального характера», утвержденным Указом Президента Российской Федерации от 06.03.1997 № 188.

Настоящее Положение определяет порядок обработки персональных данных и устанавливает общие требования к обеспечению безопасности персональных данных, обрабатываемых в федеральном государственном бюджетном образовательном учреждении высшего образования «Екатеринбургский государственный театральный институт» (далее - Оператор) как с использованием средств автоматизации, так и без использования таких средств.

В Положении используются следующие основные понятия:

автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

обезличивание персональных данных - действия, в результате которых невозможно определить без использования дополнительной информации принадлежность персональных данных конкретному субъекту персональных данных;

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;

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;

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому или иностранному юридическому лицу;

уничтожение персональных данных - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные

носители персональных данных.

Действие Положения распространяется на все структурные подразделения федерального государственного бюджетного образовательного учреждения высшего образования «Екатеринбургский государственный театральный институт».

Настоящее Положение должно быть доведено до каждого работника Оператора, осуществляющего обработку персональных данных, под роспись.

2 СУБЪЕКТЫ И ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цели обработки персональных данных, основания для их обработки, возможные действия (операции), совершаемые с персональными данными, сроки обработки и состав категорий персональных данных субъектов, обрабатываемых у Оператора, указаны в Перечне обрабатываемых персональных данных.

3 ОРГАНИЗАЦИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 Назначение ответственных лиц

Для организации обработки персональных данных у Оператора назначается ответственное лицо.

Для определения уровня защищенности информационных систем персональных данных, проверки готовности средств защиты информации к использованию, а также уничтожения персональных данных приказом руководителя Оператора назначается Комиссия по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных (далее - Комиссия).

В своей работе Комиссия руководствуется Положением о комиссии по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных, утвержденным приказом руководителя Оператора.

3.2 Допуск работников к обработке персональных данных

Допуск работников Оператора к обработке персональных данным осуществляется на основании приказа о назначении на должность в соответствии с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным.

Работники Оператора получают доступ к обработке персональных данных для выполнения ими служебных (трудовых) обязанностей, после выполнения следующих мероприятий:

- ознакомления под роспись с руководящими документами Оператора и нормативными актами Российской Федерации по обработке и обеспечению безопасности персональных данных;
- оформления письменного обязательства о неразглашении персональных данных, форма которого утверждена приказом руководителя Оператора.

Работники Оператора, имеющие допуск к персональным данным, имеют право получать только те персональные данные, которые необходимы им для выполнения служебных (трудовых) обязанностей.

3.3 Получение персональных данных

Персональные данные субъекта получаются от него самого или от него законного представителя. В случае, если персональные данные получены не от субъекта персональных данных, Оператор до начала обработки таких персональных данных обязан уведомить субъект о получении его персональных данных.

3.4 Систематизация, накопление, уточнение и использование персональных данных

Систематизация, накопление, уточнение и использование персональных данных осуществляется путем оформления и ведения документов учета и баз данных субъектов

персональных данных.

Работники Оператора, имеющие доступ к персональным данным, должны обеспечить их обработку, исключающую несанкционированный доступ к ним третьих лиц.

3.5 Передача персональных данных

Передача персональных данных субъектов третьим лицам может осуществляться только при наличии письменного согласия субъекта, если иное не предусмотрено федеральным законодательством.

При передаче персональных данных субъектов третьим лицам, с третьим лицом должно быть подписано Соглашение о соблюдении безопасности персональных данных, переданных на обработку, форма которого утверждена приказом руководителя Оператора.

Передача персональных данных субъектов между подразделениями Оператора должна осуществляться только между работниками, допущенными к обработке персональных данных.

3.6 Хранение персональных данных

Хранение персональных данных субъектов осуществляется на бумажных и машинных носителях информации в специально выделенных хранилищах подразделений Оператора, а также в информационных системах Оператора, обеспечивающих сохранность персональных данных и их защиту от несанкционированного доступа.

Уничтожение персональных данных в информационных системах, на машинных и бумажных носителях информации должно производиться в течение тридцати дней с даты достижения цели обработки (предельного срока хранения) персональных данных. При невозможности уничтожения персональных данных в течение тридцати дней с даты достижения цели обработки персональных данных, обеспечивается их блокирование и уничтожение в срок, не превышающий шести месяцев.

Порядок и правила учета, хранения и уничтожения персональных данных описаны в Регламенте по учету, хранению и уничтожению носителей персональных данных.

3.7 Уведомление об обработке персональных данных

Согласно ст. 22 ФЗ-152 Оператор уведомляет Уполномоченный орган по защите прав субъектов персональных данных об обработке персональных данных.

В случае изменения сведений, указанных в уведомлении, а также в случае прекращения обработки персональных данных Оператор также уведомляет об этом Уполномоченный орган.

4 ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

Персональные данные при их обработке без использования средств автоматизации обособляются от иной информации путем фиксации их на отдельных материальных носителях персональных данных, в специальных разделах или на полях форм (бланков).

При фиксации персональных данных на материальных носителях не допускается запись на одном материальном носителе персональных данных, цели обработки которых заведомо несовместимы. При обработке различных категорий персональных данных без использования средств автоматизации для каждой категории персональных данных должен использоваться отдельный материальный носитель.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

- типовая форма должна содержать сведения о цели обработки персональных данных, наименование и адрес Оператора, фамилию, имя, отчество и адрес субъекта

персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных - при необходимости получения письменного согласия на обработку персональных данных;

- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

Уточнение персональных данных при их обработке без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы:

- о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации;
- о категориях обрабатываемых персональных данных;
- об особенностях и правилах осуществления такой обработки.

5 ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Персональные данные обрабатываются у Оператора как с использованием средств автоматизации, так и без использования таких средств.

Порядок обработки и защиты персональных данных в информационных системах Оператора определяется Положением об обеспечении безопасности персональных данных.

Защита персональных данных от неправомерного их использования или утраты обеспечивается Оператором за счет собственных средств.

Работники Оператора, которые в рамках исполнения должностных обязанностей имеют доступ к персональным данным, обязаны соблюдать режим конфиденциальности персональных данных на всех этапах их обработки.

В отсутствие работника на его рабочем месте не должно быть документов и машинных носителей информации, содержащих персональные данные.

Доступ работников Оператора и иных лиц в помещения, в которых осуществляется обработка и хранение персональных данных, ограничивается организационными мерами и применением системы контроля и управления доступом.

Учитывая массовость и единые места обработки и хранения, гриф «конфиденциально» на документах, содержащих персональные данные, не ставится.

Организацию обработки персональных данных субъектов, контроль соблюдения мер их защиты в структурных подразделениях Оператора, сотрудники которых имеют доступ к персональным данным, осуществляют их непосредственные руководители.

Мероприятия по защите персональных данных осуществляются в соответствии с Планом мероприятий по приведению в соответствие с требованиями законодательства Российской Федерации в области персональных данных, утверждаемых руководителем Оператора.

Разработка и осуществление мероприятий по обеспечению безопасности персональных данных, обрабатываемых в информационных системах, может осуществляться сторонними организациями на договорной основе, имеющими лицензии на право проведения соответствующих работ.

6 ПОРЯДОК ОБРАБОТКИ ОБРАЩЕНИЙ И ЗАПРОСОВ ПО ВОПРОСАМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Порядок обработки запросов субъектов персональных данных описан в Регламенте по реагированию на запросы субъектов персональных данных.

Порядок обработки запросов уполномоченных органов в области персональных данных описан в Регламенте по взаимодействию с органами государственной власти в области персональных данных.

7 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Иные права и обязанности работников, в функции которых входит обработка персональных данных, определяются Инструкцией пользователя информационных систем персональных данных.

Лица, виновные в нарушении норм, регулирующих обработку и защиту персональных данных, несут материальную, дисциплинарную, административную, гражданско-правовую или уголовную ответственность в порядке, установленном федеральными законами.

Разглашение персональных данных, их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, другими локальными нормативными актами (приказами, распоряжениями) Оператора, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарного взыскания - замечания, выговора, увольнения.

Работник, имеющий доступ к персональным данным и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба работодателю (п. 7 ст. 243 ТК РФ).

Работники Оператора, имеющие доступ к персональным данным, виновные в их незаконном разглашении или использовании без согласия субъектов персональных данных из корыстной или иной личной заинтересованности и причинившие крупный ущерб, несут уголовную ответственность в соответствии со ст. 183 Уголовного кодекса Российской Федерации.

Обновление и актуализация настоящего положения осуществляется в соответствии с Регламент по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности.

Приложение № 3
к Приказу № 49-ОДУ от « 03 » апреля 2020 г

ПОЛОЖЕНИЕ
ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
федерального государственного бюджетного образовательного учреждения высшего образования «Екатеринбургский государственный театральный институт»

г. Екатеринбург, 2020 г.

СОДЕРЖАНИЕ

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.

ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Положение об обеспечении безопасности персональных данных (далее - Положение) разработано в целях выполнения требований законодательства Российской Федерации в области защиты персональных данных.

1.2. Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Екатеринбургский государственный театральный институт» (далее - Оператор).

1.3. Настоящий документ учитывает положения основных нормативных правовых актов в области защиты персональных данных, перечисленных в Положении о комиссии по приведению в соответствие с требованиями законодательства в области персональных данных.

1.4. Настоящее Положение предназначено для всех работников Оператора, а также третьих лиц, получающих временный или постоянный доступ к обрабатываемым у него ПДн на законном основании.

1.5. Настоящее Положение действует с момента его утверждения руководителем Оператора.

1.6. Актуализация настоящего Положения проводится не реже, чем два раза в год в соответствии с Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности в федеральном государственном бюджетном образовательном учреждении высшего образования «Екатеринбургский государственный театральный институт».

1.7. Внесение изменений в настоящее Положение либо утверждение его новой редакции производится на основании соответствующего приказа руководителя Оператора.

ОБЩИЕ ПОЛОЖЕНИЯ

1.8. ПДн, обрабатываемые у Оператора, цели, основание и сроки их обработки указаны в Перечне обрабатываемых персональных данных.

1.9. Обработка ПДн осуществляется Оператором с использованием средств автоматизации и без их использования.

1.10. Сроки хранения ПДн устанавливаются в письменном согласии субъекта ПДн на обработку его персональных данных, а также требованиями законодательства Российской Федерации, устанавливающими сроки хранения документов.

ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.11. Под организацией работ по обеспечению безопасности ПДн понимается формирование и всестороннее обеспечение реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от реализации угроз безопасности ПДн, и осуществляемых в целях:

- предотвращения возможных (потенциальных) угроз безопасности ПДн;
- нейтрализации и/или парирования реализуемых угроз безопасности ПДн;
- ликвидации последствий реализации угроз безопасности ПДн.

1.12. Организация работ по обеспечению безопасности ПДн у Оператора должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по обеспечению безопасности ПДн Оператором.

1.13. Задачи по приведению деятельности Оператора в соответствие с требованиями законодательства Российской Федерации в области ПДн возлагаются на специально создаваемую для этих целей Комиссию и лиц, ответственных за организацию обработки и обеспечение безопасности ПДн, которые могут быть включены в состав данной Комиссии.

1.14. В случаях, когда Оператор на основании договора поручает обработку ПДн третьему лицу, Оператору необходимо заключить с данным лицом соглашение о соблюдении безопасности персональных данных, с возложением на третье лицо обязанности по обеспечению конфиденциальности и безопасности переданных Оператором ПДн (либо включить данное обязательство в заключаемый/действующий договор).

1.15. Работы по приведению деятельности Оператора в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям: обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, и обеспечение безопасности ПДн в ИСПДн Оператора.

1.16. Работы по обеспечению безопасности ПДн, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:

- определение перечня лиц, допущенных к обработке ПДн;
- определение помещений, в которых обрабатываются персональные данные;
- информирование работников Оператора об установленных правилах обработки ПДн и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности ПДн;
- учет и защита носителей ПДн;
- разграничение доступа к носителям ПДн;
- уничтожение ПДн.

1.17. Организация и выполнение мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Оператора, осуществляются в рамках системы защиты персональных данных ИСПДн (далее - СЗПДн), развертываемой в ИСПДн в процессе ее создания или модернизации.

1.18. СЗПДн представляет собой совокупность организационных мер и технических средств защиты информации, а также используемых в ИСПДн информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности ПДн.

1.19. СЗПДн должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПДн Оператора.

1.20. Для существующих ИСПДн, в которых в процессе их создания не были предусмотрены меры по обеспечению безопасности ПДн должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению СЗПДн.

1.21. Структура, состав и основные функции СЗПДн определяются в соответствии с уровнем защищенности персональных данных, обрабатываемых в ИСПДн и моделью угроз безопасности персональных данных при их обработке в ИСПДн.

ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

1.22. В целях оценки уровня защищенности обрабатываемых у Оператора ПДн и своевременного устранения несоответствий требованиям законодательства РФ в области защиты ПДн у Оператора раз в год должен проводиться анализ изменений процессов защиты ПДн.

1.23. Анализ изменений проводится по следующим основным направлениям:

- перечень работников и третьих лиц, допущенных в обработке ПДн, степень их участия в обработке ПДн и характер взаимодействия между собой;
- перечень помещений, в которых обрабатываются персональные данные;
- перечень и объем обрабатываемых ПДн;
- цели обработки ПДн;
- процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожение ПДн;
- способы обработки ПДн (автоматизированная, неавтоматизированная);
- перечень уполномоченных органов, в рамках отношений с которыми осуществляется обработка ПДн;
- перечень программно-технических средств, используемых для обработки ПДн;
- конфигурация и топология ИСПДн в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- способы физического подключения и логического взаимодействия компонент

ИСПДн, способы подключения к сетям связи общего пользования и международного информационного обмена с определением пропускной способности линий связи;

- режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- состав используемого комплекса средств защиты ПДн и механизмов идентификации, аутентификации и разграничения прав доступа пользователей ИСПДн на уровне операционных систем, баз данных и прикладного программного обеспечения;
- перечень организационно-распорядительной документации, определяющей порядок обработки и защиты ПДн у Оператора;
- физические меры защиты ПДн, организация пропускного режима.

1.24. Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности ПДн, обрабатываемых с использованием средств автоматизации и без использования таких средств и при необходимости их уточнения.

1.25. У Оператора должен вестись учет действий, совершаемых работниками Оператора при обработке ПДн в ИСПДн. Действия с ПДн учитываются в log-файлах ИСПДн и/или в отдельной базе данных ИСПДн.

1.26. Доступ к ПДн осуществляется в соответствии с Регламентом по допуску работников и третьих лиц к обработке персональных данных, утвержденным Оператором.

1.27. Лица, допущенные к обработке ПДн, должны быть проинформированы:

- о допуске к обработке ПДн путем ознакомления с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным, обрабатываемым у Оператора;
- о категориях, обрабатываемых ПДн путем ознакомления с утвержденным Перечнем обрабатываемых персональных данных;
- о правилах осуществления обработки ПДн путем ознакомления под роспись с Положением об обработке персональных данных.

1.28. Неавтоматизированная обработка ПДн должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения материальных носителей и установить перечень лиц, допущенных к обработке ПДн. У Оператора должен вестись учет носителей ПДн.

1.29. Фиксация ПДн должна осуществляться на отдельных материальных носителях (отдельных документах). ПДн должны отделяться от иной информации.

1.30. Фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы, не допускается. В случае если на одном материальном носителе все же зафиксированы ПДн, цели обработки которых несовместимы, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

- при необходимости использования или распространения определенных ПДн осуществляется выборочное копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется);
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным выборочным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

1.31. Правила учета, хранения и уничтожения ПДн при неавтоматизированной обработке описаны в Регламенте по учету, хранению и уничтожению носителей персональных данных, утвержденном Оператором.

1.32. Должен осуществляться мониторинг фактов несанкционированного доступа к персональным данным и приниматься соответствующие меры при их обнаружении. Мониторинг осуществляется Администратором безопасности ИСПДн.

1.33. Администратором безопасности ИСПДн должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

1.34. При обработке ПДн Оператор должен иметь возможность и средства для восстановления ПДн, в случае их модификации или уничтожении вследствие несанкционированного доступа к ним. Правила резервного копирования и восстановления ПДн Оператором установлены в Регламенте по резервному копированию персональных данных, утвержденному Оператором.

1.35. Оператор определяет перечень помещений, используемых при обработке ПДн. При этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

1.36. Пользователи ИСПДн должны обеспечивать сохранность съемных носителей, содержащих ПДн. В случае утраты носителя пользователи должны немедленно сообщить об этом Администратору безопасности ИСПДн.

1.37. Если при работе с ПДн работнику Оператора необходимо покинуть рабочее место, материальные носители ПДн должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители помещаются в отведенных для хранения места.

1.38. В случае достижения цели обработки ПДн Оператор прекращает обработку ПДн или обеспечивает ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) и уничтожает ПДн или обеспечить их уничтожение (если обработка ПДн осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн. В случае если ПДн невозможно уничтожить, то они блокируются и уничтожаются в срок, не превышающий шести месяцев.

1.39. Проведение работ по созданию (модернизации) СЗПДн включает следующие стадии:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации СЗПДн;
- стадия ввода в действие СЗПДн.

1.40. На предпроектной стадии проводится определение уровня защищенности персональных данных, обрабатываемых в ИСПДн, формируется Модель угроз безопасности ПДн при их обработке в ИСПДн, разрабатывается Техническое задание на СЗПДн.

1.41. Определение уровня защищенности персональных данных, обрабатываемых в ИСПДн осуществляется в соответствии с Регламентом по определению уровня защищенности персональных данных, обрабатываемых в ИСПДн.

1.42. ИСПДн Оператора указаны в Перечне информационных систем персональных данных.

1.43. Уровень защищенности персональных данных, обрабатываемых в ИСПДн, оформляется соответствующим актом.

1.44. Модель угроз безопасности ПДн при их обработке в ИСПДн формируется на основании руководящих документов ФСТЭК России и ФСБ России.

1.45. Перечень актуальных угроз формируется для каждой ИСПДн Оператора с учетом условий функционирования ИСПДн и особенностей обработки ПДн.

1.46. По итогам определения уровня защищенности персональных данных, обрабатываемых в ИСПДн и результатам определения актуальных угроз безопасности ПДн формируются требования по обеспечению безопасности ПДн, обрабатываемых в ИСПДн. Данные требования оформляются в виде технического задания на СЗПДн.

1.47. Стадия проектирования СЗПДн включает разработку СЗПДн в составе

ИСПДн, а именно разработку разделов задания и проекта проведения по созданию (модернизации) СЗПДн в соответствии с требованиями технического задания;

1.48. Стадия реализации СЗПДн включает:

- закупку совокупности используемых в СЗПДн сертифицированных технических, программных и программно-технических средств защиты информации и их установку;
- определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением;
- разработку эксплуатационной документации на СЗПДн и СЗИ.

1.49. На стадии ввода в действие СЗПДн осуществляются:

- предварительные испытания средств защиты информации в комплексе с другими техническими и программными средствами;
- устранение несоответствий по итогам предварительных испытаний;
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПД;
- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

1.50. В процессе функционирования ИСПДн может осуществляться модернизация СЗПДн. В обязательном порядке модернизация проводится в случае, если:

- произошло изменение номенклатуры обрабатываемых ПДн, влекущее за собой изменение уровня защищенности персональных данных, обрабатываемых в ИСПДн;
- произошло изменение номенклатуры и/или актуальности угроз безопасности ПДн;
- изменилась структура ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и т.п.);
- произошло изменение законодательства Российской Федерации в области ПДн, затрагивающее вопросы обеспечения безопасности ПДн при их обработке в ИСПДн.

1.51. При возникновении условий, влияющих на безопасность ПДн (компрометация паролей, нарушение целостности и доступности персональных данных и пр.) работник Оператора обязан незамедлительно проинформировать об этом Администратора безопасности ИСПДн.

1.52. Лица, виновные в нарушении требований, предъявляемых законодательством РФ к защите ПДн, несут гражданскую, уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

Приложение № 4
к Приказу №49-ОД от «03» апреля 2020 г.

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

федерального государственного бюджетного образовательного учреждения высшего образования «Екатеринбургский государственный театральный институт»

г. Екатеринбург, 2020 г.

СОДЕРЖАНИЕ

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 федеральном государственном бюджетном образовательном учреждении высшего образования «Екатеринбургский государственный театральный институт» (далее – ЕГТИ).

2.2. Определение уровня защищенности ПДн, обрабатываемых в ИСПДн, в ЕГТИ возлагается на Комиссию по приведению ЕГТИ 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;	Негативные последствия	Средняя опасность
- жизнь и здоровье субъекта ПДн не затронуты; - основные интересы и права субъекта ПДн, закрепленные Конституцией РФ, не затронуты.		
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

федерального государственного бюджетного образовательного учреждения высшего образования «Екатеринбургский государственный театральный институт»

С ТРЕБОВАНИЯМИ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

г. _____ «__»_____2020 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 федеральном государственном бюджетном образовательном учреждении высшего образования «Екатеринбургский государственный театральный институт», 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	