МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ
(национальный исследовательский университет)» (МАИ)

П Р И К А З

17.03.2022 № 148

МОСКВА

Об утверждении Положения об организации работы с персональными данными в МАИ

Во исполнение Федерального закона от 27.07.2006 № 152 - ФЗ «О персональных данных», а также постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также приказа МАИ от 17.03.2022 № 147 «О назначении ответственных лиц за организацию работы с персональными данными в МАИ»

П Р И К А З Ы В А Ю:

1. Ввести в действие с 13.05.2022 Положение об организации работы с персональными данными в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский авиационный институт (национальный исследовательский университет)» (МАИ) (далее - Положение) (Приложение 1).

2. Руководителям структурных подразделений университета, в том числе обособленных, ознакомить под подпись работников и обучающихся своего подразделения с Положением в срок до 17.06.2022, а также обеспечить реализацию норм Положения в установленном порядке.

3. Контроль исполнения настоящего приказа возложить на Директора Департамента организационной и кадровой работы Сорокина А.Е.

Ректор М.А. Погосян

Проект приказа вносит:
Помощник ректора, начальник
Управления делами Департамента
организационной и кадровой работы
А.В. Макаренко

Согласовано:
Директор Департамента организационной и кадровой работы А.Е. Сорокин

Директор Департамента информационных технологий С.С. Попов

Начальник Правового управления М.В. Васильев

Начальник ОРД М.А. Попова

Приложение № 1
к приказу от 17.03.2022 г. № 148

ПОЛОЖЕНИЕ

об организации работы с персональными данными в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский авиационный институт (национальный исследовательский университет)» (МАИ)

Москва, 2022 год

1. Общие положения

1.1. Настоящее Положение по обработке персональных данных (далее - Положение) в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский авиационный институт (национальный исследовательский университет)» (далее – МАИ) разработано в соответствии с Трудовым кодексом Российской Федерации, Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

1.2. Цель разработки Положения – определение порядка обработки персональных данных в МАИ; обеспечение 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, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с момента его утверждения ректором МАИ и действует бессрочно, либо до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом ректора МАИ.

1.4. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения, если иное не определено законом.

1.5. Настоящее Положение разработано для реализации следующих задач:

- регламентации порядка осуществления операций с персональными данными субъектов персональных данных МАИ;
- обеспечения требований закона № 152-ФЗ и иных нормативно-правовых актов, регулирующих обработку персональных данных;
- установления полномочий, прав и обязанностей субъектов МАИ в части работы с персональными данными;
- установления механизмов ответственности работников МАИ за нарушение локальных нормативно-правовых актов, а также положений действующего законодательства, регулирующего использование персональных данных.

2. Основные понятия и состав персональных данных

2.1. В настоящем Положении используются следующие термины и их определения:

Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (далее – ИСПДН).

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не

допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания, если иное не предусмотрено федеральным законом.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа к персональным данным.

Обработка персональных данных – действия (операции) 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.

Технические средства информационной системы персональных данных– средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе 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.

Уровень защищенности персональных данных – комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, либо без использования средств автоматизации.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Целостность информации – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения).

3. Полномочия, права и обязанности ответственных лиц

3.1. Полномочия ответственных лиц:

3.1.1. Организовывать принятие правовых, организационных и технических мер для обеспечения защиты персональных данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий.

3.1.2. Организовывать и осуществлять внутренний контроль за соблюдением уполномоченными на обработку персональных данных требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных.

3.1.3. Организовывать доведение до сведения уполномоченных на обработку персональных данных положений законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

3.1.4. Организовывать прием и обработку обращений и запросов субъектов персональных данных, а также осуществлять контроль за приемом и обработкой таких обращений и запросов.

3.1.5. В случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

3.1.6. Осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

3.1.7. Доводить до сведения субъектов персональных данных оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

3.1.8. Блокировать неправомерно обрабатываемые персональные данные, прекращать обработку персональных данных в соответствии с законодательством Российской Федерации.

3.1.9. Уведомлять субъектов персональных данных об устранении допущенных нарушений при обработке их персональных данных.

3.1.10. Проводить оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства Российской Федерации о

персональных данных, соотношения указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных законодательством Российской Федерации в области обработки и защиты персональных данных.

3.1.11. Участвовать в рассмотрении проектов решений по вопросам своей компетенции.

3.1.2. Особые полномочия ответственного лица за организацию работы с персональными данными:

3.1.2.1. Ответственное лицо в целом за организацию работы с персональными данными в МАИ обладает всеми перечисленными полномочиями, определенными в п.3.1.1-3.1.11, а также руководит и координирует деятельностью структурных подразделений по вопросам обработки персональных данных.

3.1.2.2. Ответственное лицо в целом за организацию работы с персональными данными в МАИ наделено особым правом в случае установления нарушения работниками настоящего Положения выносить Предписание о выявлении нарушений при работе с персональными данными в отношении работников, имеющих доступ к персональным данным (далее – Предписание) (Приложение 1).

3.1.2.3. Ответственное лицо в целом за организацию работы с персональными данными в МАИ имеет право вносить предложения для применения мер дисциплинарного или материального характера к виновным лицам, в отношении которых было вынесено Предписание, в соответствии с действующим законодательством.

3.2. Ответственные лица имеют право:

3.2.1. Требовать от работников МАИ выполнения локальных нормативно-правовых актов в части работы с персональными данными.

3.2.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.2.3. Проводить служебные проверки и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.2.4. Проводить расследование по случаям несанкционированного доступа к персональным данным и другим случаям нарушения режима обработки персональных данных.

3.2.5. Вносить предложения по применению дисциплинарных взысканий к работникам, нарушившим требования Положения и других локальных нормативных документов МАИ в области обработки и защиты персональных данных.

3.2.6. Знакомиться с проектными решениями руководства, касающимися его деятельности.

3.2.7. Вносить предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

3.2.8. В пределах своей компетенции сообщать ответственному лицу за обработку персональных данных о недостатках, выявленных в процессе исполнения должностных обязанностей, и вносить предложения по их устранению.

3.2.9. Привлекать с разрешения ответственного лица за обработку персональных данных работников всех структурных подразделений к решению задач, предусмотренных настоящим Положением.

3.2.10. Запрашивать информацию и документы, необходимые для выполнения задач, предусмотренных настоящим Положением, у работников всех структурных подразделений МАИ.

3.2.11. Представлять на рассмотрение руководителя предложений по вопросам деятельности МАИ в области обработки персональных данных.

3.2.12. Иметь доступ к информации, касающейся обработки персональных данных на любых видах информационных и бумажных носителях.

3.2.13. Принимать неотложные меры по защите персональных данных.

3.3. Ответственные лица обязаны:

3.3.1. Соблюдать требования законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, Правил обработки персональных данных и других локальных нормативных документов МАИ в области обработки и защиты персональных данных.

3.3.2. Доводить до сведения работников МАИ положения законодательства Российской Федерации о персональных данных, Положения и других локальных нормативных документов МАИ по вопросам обработки и требований к защите персональных данных.

3.3.3. Проводить инструктажи и занятия по изучению правовой базы по защите персональных данных с работниками МАИ, имеющими доступ к персональным данным.

3.3.4. Оказывать консультационную помощь работникам по применению средств защиты персональных данных.

3.3.5. Осуществлять контроль соблюдения в МАИ законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, и настоящего Положения на соответствие обработки персональных данных к требованиям о защите персональных данных

3.3.6. Проводить регулярные внутренние проверки, согласно Плану внутренних проверок контроля соответствия обработки, персональных данных требованиям к защите персональных данных.

3.3.7. Участвовать в проведении расследований случаев несанкционированного доступа к персональным данным и других нарушений Положения.

3.3.8. Составлять и предлагать на утверждение ректору МАИ перечень лиц и объема их полномочий, которым разрешен доступ к персональным данным.

3.3.9. Не допускать к работе с персональными данными лиц, не обладающих для этого соответствующими правами.

3.3.10. Осуществлять регистрацию обращений и запросов субъектов персональных данных или их представителей в Журнале учёта обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных о выполнении их законных прав (Приложение 2).

4. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

4.1. Ответственные лица за организацию обработки персональных данных несут ответственность:

4.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящим Положением, в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.1.2. За правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.1.3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Ответственность работников МАИ в части работы с персональными данными:

4.2.1. Работники МАИ, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, также несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

4.2.2. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

5. Порядок организации и проведения работ по обеспечению безопасности персональных данных

5.1. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн или в бумажном виде, понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн, реализуемых в рамках создаваемой системы защиты персональных данных (далее – СЗПДн).

5.2. СЗПДн включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности ПДн, уровня защищенности ПДн, который необходимо обеспечить, и информационных технологий, используемых в информационных системах или без использования таковых.

5.3. Безопасность ПДн при их обработке в ИСПДн обеспечивает.

5.4. Выбор средств защиты информации для СЗПДн осуществляется МАИ в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации (далее – ФСБ России) и Федеральной службой по техническому и экспортному контролю (далее – ФСТЭК России) во исполнение Федерального закона «О персональных данных».

5.5. Структура, состав и основные функции СЗПДн определяются исходя из уровня защищенности ПДн при их обработке в ИСПДн.

5.6. СЗПДн создается в три этапа:

Этап 1. Предпроектное обследование ИСПДн и разработка технического задания на создание СЗПДн.

Этап 2. Проектирование СЗПДн, закупка, установка, настройка необходимых средств защиты информации.

Этап 3. Ввод ИСПДн с СЗПДн в эксплуатацию.

5.7. Этап 1. Проведение предпроектного обследования и разработка технического задания на создание СЗПДн.Назначение ответственного за организацию обработки ПДн МАИ.

5.7.2. Создание комиссии по определению уровня защищенности ПДн при их обработке в ИСПДн МАИ.

5.7.3. Определение целей обработки ПДн МАИ.

5.7.4. Определение перечня ИСПДн МАИ и состава ПДн, обрабатываемых в ИСПДн.

5.7.5. Определение перечня обрабатываемых МАИ ПДн.

5.7.6. Определение сроков обработки и хранения ПДн, исходя из требования, что ПДн не должны храниться дольше, чем этого требуют цели обработки этих ПДн, по достижению которых ПДн подлежат уничтожению.

5.7.7. Определение перечня используемых в ИСПДн (предлагаемых к использованию в ИСПДн) общесистемных и прикладных программных средств.

5.7.8. Определение режимов обработки ПДн в ИСПДн в целом и в отдельных компонентах.

5.7.9. Назначение ответственного за обеспечение безопасности ПДн в ИСПДн (далее – Ответственный) для разработки и осуществления технических мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн.

5.7.10. Назначение ответственного пользователя криптосредств, обеспечивающего функционирование и безопасность криптосредств, предназначенных для обеспечения безопасности ПДн. Утверждение перечня лиц, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности ПДн в ИСПДн (пользователей криптосредств).

5.7.11. Определение перечня помещений, в которых размещены ИСПДн и материальные носители ПДн.

5.7.12. Определение конфигурации и топологии ИСПДн в целом и их отдельных компонент, физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня и назначения.

5.7.13. Определение технических средств и систем, используемых в ИСПДн, включая условия их расположения.

5.7.14. Формирование технических паспортов ИСПДн.

5.7.15. Разработка организационно-распорядительных документов (далее – ОРД), регламентирующих процесс обработки и защиты ПДн:

– Политика в отношении обработки персональных данных;

– Положение об обработке ПДн в МАИ.

5.7.16. Получение (при необходимости) согласия на обработку ПДн субъектом ПДн, подписание обязательства о соблюдении конфиденциальности ПДн.

5.7.17. Утверждение форм уведомлений субъектов ПДн и форм журналов, необходимых в целях обеспечения безопасности ПДн.

5.7.18. Определение уровня защищенности ПДн при их обработке в ИСПДн в соответствии с требованиями постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (подготовка и

утверждение акта определения уровня защищенности ПДн при их обработке в ИСПДн).

5.7.19. Определение типа угроз безопасности ПДн, актуальных для информационной системы, с учетом оценки возможного вреда в соответствии с нормативными правовыми актами, принятыми во исполнение Федерального закона «О персональных данных» от 27 июля 2006 г. № 152. Определение угроз безопасности ПДн в конкретных условиях функционирования ИСПДн (разработка моделей угроз безопасности ПДн при их обработке в ИСПДн).

5.7.20. Формирование технического задания на разработку СЗПДн по результатам предпроектного обследования на основе нормативно-методических документов ФСТЭК России и ФСБ России с учетом установленного уровня защищенности ПДн при их обработке в ИСПДн.

Техническое задание на разработку СЗПДн должно содержать:

– обоснование разработки СЗПДн;

– исходные данные создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

– уровень защищенности ПДн при их обработке в ИСПДн;

– ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПДн, и приниматься в эксплуатацию ИСПДн;

– конкретизацию мероприятий и требований к СЗПДн;

– состав и содержание работ по этапам разработки и внедрения СЗПДн;

– перечень предполагаемых к использованию сертифицированных средств защиты информации.

5.8. Этап 2. Проектирование СЗПДн, закупка, установка, настройка и опытная эксплуатация необходимых средств защиты информации.Создание СЗПДн является необходимым условием обеспечения безопасности ПДн, в том случае, если существующие организационные и технические меры обеспечения безопасности не соответствуют требованиям к обеспечению безопасности ПДн для соответствующего уровня защищенности ПДн при их обработке в ИСПДн и (или) не нейтрализуют всех угроз безопасности ПДн для данной ИСПДн.

5.8.2. Технические меры защиты ПДн предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предпроектного обследования информационных ресурсов МАИ. Применение технических мер должно быть регламентировано локальным актом МАИ.

5.8.3. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

5.8.4. На стадии проектирования и создания СЗПДн для ИСПДн МАИ проводятся следующие мероприятия:

– разработка технического проекта СЗПДн;

– приобретение (при необходимости), установка и настройка серийно выпускаемых технических средств обработки, передачи и хранения информации;

– разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

– приобретение, установка и настройка сертифицированных технических, программных и программно-технических средств защиты информации, в том числе (при необходимости) средств криптографической защиты информации;

– реализация разрешительной системы доступа пользователей ИСПДн к обрабатываемой в ИСПДн информации;

– подготовка эксплуатационной документации на используемые средства защиты информации;

– корректировка (дополнение) организационно-распорядительной документации в части защиты информации.

5.9. Этап 3. Ввод ИСПДн с СЗПДн в промышленную эксплуатацию.На стадии ввода в ИСПДн (СЗПДн) осуществляются:

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн (при необходимости);

– приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации (при необходимости);

– контроль выполнения требований (возможно проведение данного контроля в виде аттестации по требованиям безопасности ПДн).

5.9.2. Контроль за выполнением настоящих требований организуется и проводится МАИ (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые МАИ (уполномоченным лицом).

6. Проведение работ по обеспечению безопасности персональных данных

6.1. Работы по обеспечению безопасности ПДн проводятся в соответствии с Планом мероприятий по защите персональных данных (Приложение 3). Внутренние проверки режима обработки и защиты ПДн МАИ проводятся в соответствии с Планом внутренних проверок режима обработки и защиты персональных данных (Приложение 4). По результатам проведения внутренней проверки составляется Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в МАИ (Приложение 5).

6.2. Контроль за проведением работ по обеспечению безопасности ПДн осуществляет ответственный за организацию обработки ПДн в виде методического руководства, участия в разработке требований по защите ПДн, организации работ по выявлению возможных каналов утечки информации, согласования выбора средств вычислительной техники и связи, технических и программных средств защиты, участия в оценке соответствия ИСПДн МАИ требованиям безопасности ПДн.

6.3. При необходимости к проведению работ по обеспечению безопасности ПДн могут привлекаться специализированные организации, имеющие лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

6.4. В соответствии с Постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)», при необходимости использования при создании СЗПДн средств криптографической защиты информации к проведению работ по обеспечению безопасности ПДн МАИ необходимо привлекать специализированные организации, имеющие лицензии ФСБ России на осуществление работ по распространению шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведения, составляющие государственную тайну, на осуществление технического обслуживания шифровальных (криптографических) средств, на осуществление работ по оказанию услуг в области шифрования информации, не содержащих сведений, составляющих государственную тайну.

Приложение 1
к Положению об организации работы с персональными данными в МАИ от «17» 05 2022.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ

(национальный исследовательский университет)» (МАИ)

ПРЕДПИСАНИЕ

ответственного лица за организацию работы с персональными данными

«__» _____ _____г. №____

Кому: _____
(ФИО работника, должность, наименование подразделения и др.)

В соответствии со статьями 90 Трудового кодекса Российской Федерации «Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника», статьей 152 Трудового кодекса Российской Федерации «Дисциплинарные взыскания»,

предлагаю дать письменные объяснения по следующим выявленным нарушениям при работе с персональными данными:

№ п/п	Перечень выявленных нарушений	Срок для устранения нарушения	Особые отметки (повторное нарушение)

О выполнении настоящего предписания прошу сообщить ответственному лицу за организацию обработки и хранения персональных данных, осуществляемых без/с использования/ем средств автоматизации в срок до 1 рабочего дня со дня ознакомления с настоящим предписанием.

Ответственное лицо за организацию работы
с персональными данными _____ (Ф.И.О.)

Ответственное лицо за организацию обработки
и хранения персональных данных, осуществляемых
без/с использования/ем средств автоматизации _____(Ф.И.О.)

Предписание получил: _____/_____/_____
(ФИО работника, должность, подразделение, дата)

Приложение 2

к Положению об организации работы с персональными данными в МАИ от «14» 03 2024 г.

Разработал:
Помощник ректора, ответственный
за обработку персональных данных в МАИ
А.В. Макаренко _____

ЖУРНАЛ УЧЕТА ОБРАЩЕНИЙ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ О ВЫПОЛНЕНИИ ИХ ЗАКОННЫХ ПРАВ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Журнал начат «___» _____ _____г.

Ответственный за ведение:

_____ (должность)

_____ (Ф.И.О.)

_____(подпись.)

Журнал окончен «___» _____ _____г.

_____(должность)

_____ (Ф.И.О.)

_____ (подпись.)

Приложение 3

к Положению об организации работы с персональными данными в МАИ от «17» 03 2022 г.

План мероприятий по защите персональных данных в МАИ

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
1.	Документальное регламентирование работы с ПДн	При необходимости	Разработка организационно-распорядительных документов по защите ПДн, либо внесение изменений в существующие
2.	Получение согласий субъектов ПДн (физических лиц) на обработку ПДн в случаях, когда этого требует законодательство	Постоянно	В случаях, предусмотренных Федеральным законом «О персональных данных», обработка ПДн осуществляется только с согласия в письменной форме субъекта ПДн. Форма согласия приведена в Приказе «Об утверждении форм документов, необходимых в целях выполнения требований законодательства в области персональных данных». Равнозначным содержащему собственноручную подпись субъекта ПДн согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью
3.	Пересмотр договора с третьими лицами на поручение обработки ПДн	При необходимости	В случае поручения обработки ПДн субъектов ПДн третьим лицам (например, кредитно-финансовым учреждениям) в договор включается пункт о соблюдении конфиденциальности при обработке ПДн, а также учитываются требования ч.3 ст.6 Федерального закона «О персональных данных»
4.	Ограничение доступа сотрудников к ПДн	При необходимости (при создании ИСПДн)	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствие с требованиями закона необходимо разграничить доступ сотрудников Московского Авиационного Института к ПДн
5.	Взаимодействие с субъектами ПДн	Постоянно	Работа с обращениями субъектов ПДн, ведение журналов учета передачи персональных данных, обращений субъектов ПДн, уведомление субъектов ПДн об уничтожении, изменении, прекращении обработки, устранении нарушений, допущенных при обработке ПДн, получении ПДн от третьих лиц

№ п/п	Наименование мероприятия	Срок выполнения	Примечание
6.	Ведение журналов учета электронных носителей персональных данных, средств защиты информации	Постоянно	
7.	Повышение квалификации сотрудников в области защиты ПДн	Постоянно	Повышение квалификации сотрудников, ответственных за выполнение работ – не менее раза в три года, повышение осведомленности сотрудников – постоянно (данное обучение проводит ответственный за обеспечение безопасности ПДн в ИСПДн)
8.	Инвентаризация информационных ресурсов	Раз в полгода	Проводится с целью выявления в информационных ресурсах присутствия ПДн
9.	Установка сроков обработки ПДн и процедуры их уничтожения по окончании срока обработки	При необходимости	Для уничтожения ПДн Московским Авиационным Институтом устанавливаются сроки обработки ПДн, которые документально подтверждаются в локальных актах Московского Авиационного Института. При пересмотре сроков необходимые изменения вносятся в соответствующие документы
10.	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн	При необходимости	Уничтожение электронных (бумажных) носителей информации при достижении целей обработки ПДн производится с оформлением Акта на списание и уничтожение электронных (бумажных) носителей информации. Форма соответствующего акта приведена в Приказе «О комиссии по уничтожению персональных данных»
11.	Определение уровня защищенности ПДн при их обработке в ИСПДн	При необходимости	Определение уровня защищенности ПДн при их обработке в ИСПДн осуществляется при создании ИСПДн, при изменении состава ПДн, объема обрабатываемых ПДн, субъектов ПДн
12.	Выявление угроз безопасности и разработка моделей угроз и нарушителя	При необходимости	Разрабатывается при создании системы защиты ИСПДн
13.	Аттестация ИСПДн на соответствие требованиям по обеспечению безопасности ПДн	При необходимости	Проводится совместно с лицензиатами ФСТЭК
14.	Эксплуатация ИСПДн и контроль безопасности ПДн	Постоянно	
15.	Понижение требований по защите ПДн путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ и прочих доступных мер	При необходимости	В случае создания ИСПДн, а также приведения имеющихся ИСПДн в соответствии с требованиями закона

Приложение 4
к Положению об организации работы с персональными данными в МАИ от «17» 03 2021 г.

План внутренних проверок режима обработки и защиты персональных данных в МАИ

№	Мероприятие	Периодичность	Дата, подпись исполнителя
1.	Осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн ФЗ-152 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам	Раз в полгода	
2.	Проверка ознакомления сотрудников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн	Раз в полгода	
3.	Проверка получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство	Раз в полгода	
4.	Проверка подписания сотрудниками, осуществляющими обработку ПДн, основных форм, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПДн: - Уведомления о факте обработки ПДн без использования средств автоматизации; - Обязательства о соблюдении конфиденциальности ПДн; - Формы ознакомления с положениями законодательства Российской Федерации о ПДн, локальными актами МАИ по вопросам обработки ПДн; - Разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн	Раз в полгода	
5.	Проверка уничтожения материальных носителей ПДн с составлением соответствующего акта	Ежегодно	
6.	Проверка ведения журналов по учету обращений субъектов ПДн и учету передачи ПДн субъектов третьим лицам	Раз в полгода	
7.	Проведение внутренних проверок на предмет выявления изменений в правилах обработки и защиты ПДн	Ежегодно	
8.	Проверка соблюдения условий хранения материальных носителей ПДн	Раз в полгода	
9.	Проверка состояния актуальности Уведомления об обработке (намерении осуществлять обработку) ПДн	Раз в полгода	
10.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику МАИ в отношении обработки ПДн	Раз в полгода	
11.	Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также анализ и выявление новых, еще неизвестных, угроз	Ежегодно	
12.	Оценка вреда, который может быть причинен субъектам ПДн в случае нарушения ФЗ-152 «О персональных данных»	Ежегодно	
13.	Проверка применения для обеспечения безопасности ПДн средств защиты информации, прошедших в установленном порядке процедуру соответствия	Раз в полгода	
14.		При	

№	Мероприятие	Периодичность	Дата, подпись исполнителя
	Оценка эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию ИСПДн	необходимости	
15.	Контроль учета машинных носителей ПДн	Раз в полгода	
16.	Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ПДн в ИСПДн	Раз в полгода	
17.	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИСПДн	Ежеквартально	
18.	Контроль внесения изменений в структурно-функциональные характеристики ИСПДн	Ежеквартально	
19.	Контроль корректности настроек средств защиты информации	Раз в полгода	
20.	Контроль за обеспечением резервного копирования	Ежеквартально	
21.	Поддержание в актуальном состоянии организационно-распорядительных документов по вопросам защиты ПДн	Раз в полгода	

Приложение 5

к Положению об организации работы с персональными данными в МАИ от «17» 03 2022г.

Отчет о результатах проведения внутренней проверки режима обработки и защиты персональных данных в МАИ

1.1 Внутренняя проверка произведена на основании Положения по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МАИ от «__» _____20__г.

1.2 Проверка проводилась «___»_____20__ г. по адресу:

_____

_____

1.3 В ходе проверки были проведены следующие мероприятия:

1) _____
2) _____
3) _____
4) _____
5) _____

1.4 Результаты проведения проверки:

1) _____
2) _____
3) _____
4) _____
5) _____

1.5 Необходимые мероприятия.

На основании проведения внутренней проверки режима обработки и защиты ПДн рекомендуется осуществить следующие мероприятия:

1) _____
2) _____
3) _____
4) _____
5) _____

Подписи ответственных лиц, проводивших внутреннюю проверку режима обработки и защиты ПДн:

_____ (дата)	_____ (подпись)	_____ (расшифровка подписи)
_____ (дата)	_____ (подпись)	_____ (расшифровка подписи)
_____ (дата)	_____ (подпись)	_____ (расшифровка подписи)