МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»
(УУНиТ)

ПРИКАЗ

20.10.2025 № 2907

Уфа

Об утверждении Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Уфимский университет науки и технологий»

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, п р и к а з ы в а ю:

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Уфимский университет науки и технологий» (приложение).

2. Управлению цифровой трансформации (Ефимов И.С.) произвести опубликование настоящего приказа и приложения к нему на официальном сайте УУНиТ в разделе «Защита персональных данных» и в Правовой базе УУНиТ.

3. Руководителям структурных подразделений ознакомить под подпись с настоящим приказом работников, допущенных к обработке персональных данных.

4. Общему отделу обеспечить рассылку настоящего приказа проректорам и во все структурные подразделения УУНиТ, в том числе в филиалы.

5. Контроль за исполнением настоящего приказа возложить на проректора по цифровой трансформации Хайбуллина А.Р.

Ректор В.П. Захаров

ДОКУМЕНТ ПОДПИСАН УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
42B2468CE6E0BD2F3D43778DD30EC01D8F301D38
Владелец:Захаров Вадим Петрович
Документ подписан: 20-10-2025 10:45:12
Действителен с 2024-9-9 12:33:19 по 2025-12-3 12:33:19

Приложение к приказу
от 20.10.2025 № 2907

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Уфимский университет науки и технологий»

1. Общие положения

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) определяют в федеральном государственном бюджетном образовательном учреждении высшего образования «Уфимский университет науки и технологий» (далее – УУНиТ) основания и порядок осуществления внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Политике УУНиТ в отношении обработки персональных данных, локальным нормативным актам УУНиТ.

1.2. Перечень нормативных правовых актов, на основании которых разработаны Правила:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);

– постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (далее – постановление Правительства РФ № 687);

– постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – постановление Правительства РФ № 1119);

– приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

– приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»»;

– приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных»;

– приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 №180 «Об утверждении форм уведомлений о намерении осуществлять обработку персональных данных, об изменении сведений, содержащихся в уведомлении о намерении осуществлять обработку персональных данных, о прекращении обработки персональных данных»;

– приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер

по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – приказ ФСТЭК России № 21);

– приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну» (далее – приказ ФСТЭК России № 77).

1.3. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных статьей 3 Федерального закона № 152-ФЗ.

2. Основания проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

2.1. Основаниями для проведения внутреннего контроля являются требования пункта 4 части 1 статьи 18.1., пункта 1 части 4, статьи 22.1. Федерального закона № 152-ФЗ, пункта 17 требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ № 1119, ежегодный план внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных, утверждаемый ректором УУНиТ.

2.2. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) осуществляется в УУНиТ путем проведения проверок соблюдения требований законодательства в сфере персональных данных и внутренних документов УУНиТ по обработке и защите персональных данных.

2.3. Организация разработки проекта ежегодного плана внутренних проверок обеспечивается ответственным за организацию обработки персональных данных в УУНиТ.

2.4. В случае проведения оценки соответствия информационной системы персональных данных требованиям по защите информации в форме аттестации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, обеспечивается проведение периодического контроля уровня защиты информации, результаты которого оформляются протоколами и отражаются в Техническом паспорте информационной системы персональных данных. Протоколы контроля защиты информации аттестованной информационной системы персональных данных не реже 1 раза в 2 года предоставляются в территориальный орган ФСТЭК России.

Непредставление протоколов контроля защиты информации в территориальный орган ФСТЭК России является основанием для приостановления действия аттестата соответствия информационной системы персональных данных требованиям по защите информации.

3. Порядок осуществления внутреннего контроля

3.1. Внутренний контроль проводится самостоятельно УУНиТ и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.2. Для проведения внутреннего контроля в УУНиТ создается комиссия по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Комиссия).

3.3. Состав Комиссии, как правило, состоящий из не менее трех работников УУНиТ, утверждается приказом ректора.

3.4. Председателем Комиссии, как правило, назначается ответственный за организацию обработки персональных данных в УУНиТ.

3.5. Все члены комиссии при принятии решения обладают равными правами.

3.6. Члены Комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения внутреннего контроля, обеспечивают конфиденциальность персональных данных субъектов персональных данных.

3.7. Комиссия при проведении проверки обязана:

3.7.1. Провести анализ реализации мер, направленных на обеспечение выполнения УУНиТ обязанностей, предусмотренных статьями 18.1, 19 Федерального закона № 152-ФЗ и принятыми в соответствии с ним локальными нормативными актами в отношении обработки персональных данных, и проверить:

- наличие актуального приказа о назначении лица, ответственного за организацию обработки персональных данных в УУНиТ, утвержденной инструкции ответственного за организацию обработки персональных данных в УУНиТ, а также внесение соответствующих дополнений в должностную инструкцию работника, назначенного ответственным за организацию обработки персональных данных УУНиТ;

- актуальность уведомления о намерении осуществлять обработку персональных данных, направленного в уполномоченный орган по защите прав субъектов персональных данных;

- актуальность Политики в отношении обработки персональных данных в УУНиТ, утвержденной приказом УУНиТ (далее - Политика), и обеспечение неограниченного доступа к Политике и сведениям о реализуемых требованиях к защите персональных данных, в том числе размещение их на официальном сайте УУНиТ в информационно-телекоммуникационной сети;

– наличие и актуальность Перечня персональных данных по каждой категории персональных данных, обрабатываемых в УУНиТ, и Перечня информационных систем персональных данных в УУНиТ;

– наличие правовых оснований для обработки персональных данных по каждой категории субъектов персональных данных, независимо от способа обработки персональных данных;

– соответствие целей обработки персональных данных содержанию и объему обрабатываемых персональных данных, независимо от способа их обработки;

– оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ (далее – оценка вреда), соотношение указанного вреда и принимаемых мер, направленных на обеспечение выполнения УУНиТ обязанностей, предусмотренных Федеральным законом № 152-ФЗ. В случае необходимости по результатам проверки оценки вреда оформляется соответствующий акт, форма которого утверждается приказом УУНиТ;

– ознакомление работников (документально подтвержденное), непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику УУНиТ в отношении обработки персональных данных, локальными нормативными актами по вопросам обработки и обеспечения безопасности персональных данных;

– соответствие установленных прав доступа к персональным данным в информационной системе (системах) персональных данных трудовым обязанностям работников УУНиТ;

– наличие и полноту заполнения работниками УУНиТ обязательств о соблюдении конфиденциальности персональных данных, документа об информировании о факте обработки персональных данных без использования средств автоматизации, разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные;

– наличие согласий субъектов персональных данных на обработку персональных данных и разъяснений субъекту персональных данных юридических последствий отказа предоставить свои персональные данные в случаях, когда этого требует законодательство Российской Федерации;

– наличие и ведение Журнала обращений субъектов персональных данных и представителей субъектов персональных данных, соблюдения процедур и сроков подготовки ответов на обращения субъектов персональных данных, а также учета предоставления персональных данных субъектов персональных данных по письменным запросам третьих лиц в порядке, установленном действующим законодательством Российской Федерации;

– наличие (в случае заключения соответствующего договора) в поручении на обработку персональных данных: перечня действия (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанности соблюдения конфиденциальности персональных данных, обеспечения безопасности персональных данных при их обработке, а также требований к защите обрабатываемых персональных данных со статьей 19 Федерального закона № 152-ФЗ;

– актуальность Перечня мест хранения материальных носителей персональных данных и обеспечение контроля хранения материальных носителей персональных данных в условиях, исключающих несанкционированный доступ к ним, а также обеспечение раздельного хранения персональных данных в случаях их обработки без использования средств автоматизации при несовместимости целей обработки персональных данных;

– соблюдение сроков хранения и порядка уничтожения персональных данных в информационных системах персональных данных, материальных носителей персональных данных, а также персональных данных на носителях информации в соответствии с локальными нормативными актами УУНиТ;

– актуальность организационно-распорядительных документов по вопросам обработки персональных данных.

3.7.2. Проанализировать выполнение в УУНиТ требований по определению и обеспечению уровня защищенности персональных данных при их обработке в информационной системе персональных данных, утвержденных постановлением Правительства РФ № 1119, и проверить:

– соответствие указанных в утвержденном в УУНиТ Перечне обрабатываемых персональных данных в информационной системе персональных данных категорий персональных данных, категорий субъектов персональных данных и количества субъектов персональных данных фактически обрабатываемым в информационной системе персональным данным;

– соответствие фактического типа актуальных угроз безопасности персональных данных в информационной системе персональных данных с учетом оценки возможного вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, типу актуальных угроз безопасности персональных данных, указанному в утвержденном в УУНиТ Акте классификации информационной системы персональных данных (в случае, если проводились работы по аттестации информационной системы персональных данных) либо в акте определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных (в случае, если работы по аттестации информационной системы персональных данных не проводились);

– назначение работника, ответственного за обеспечение безопасности персональных данных в информационной системе персональных данных;

– соответствие Перечня помещений, в которых размещена информационная система персональных данных, утвержденного в УУНиТ, фактическому размещению оборудования информационной системы персональных данных, включая средства защиты информации;

– соответствие Перечня лиц, имеющих доступ к персональным данным в связи с исполнением своих трудовых (служебных) обязанностей Перечню лиц, имеющих доступ в помещения, в которых размещена информационная система персональных данных, утвержденного в УУНиТ, фактически находящимся в указанных помещениях на момент проверки;

– фактическое выполнение организационных и технических мер по обеспечению безопасности помещений, в которых размещена информационная система персональных данных, препятствующих возможности неконтролируемого проникновения или пребывания в указанных помещениях лиц, не имеющих права доступа в них (при наличии - фактическое опечатывание входных дверей указанных помещений, применение систем контроля и управления доступом, средств охранной сигнализации, систем видеонаблюдения, оборудование оконных проемов первых и последних этажей здания, где размещено оборудование информационной системы персональных данных, запирающимися ставнями и т.д.);

– наличие сертификатов соответствия требованиям безопасности информации на все используемые средства защиты информации, фактически используемые в УУНиТ;

– обеспечение сохранности машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные в информационной системе персональных данных путем проведения сверки соответствия количества учтенных носителей фактическому, а также сверки заводских и учетных номеров, фактической проверки условий хранения и использования машинных носителей персональных данных.

3.7.3. Проанализировать состояние работы в УУНиТ по реализации состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России № 21 и проверить:

– фактическую реализацию установленного в УУНиТ порядка идентификации и аутентификации пользователей информационной системы персональных данных;

– реализацию процесса управления доступом к ресурсам информационной системы персональных данных;

– регистрацию событий информационной безопасности в информационной системе персональных данных в соответствии с Инструкцией по управлению событиями информационной безопасности;

– реализацию выявления инцидентов информационной безопасности и реагирования на них при наличии запланированных работ по аттестации информационной системы персональных данных;

– организацию антивирусной защиты в информационной системе персональных данных и регулярность обновления базы данных признаков вредоносных программ (вирусов);

– реализацию выявления, анализа и устранения уязвимостей в информационной системе персональных данных при наличии запланированных работ по проведению аттестации информационной системы персональных данных;

– установку обновлений программного обеспечения, в том числе обновление программного обеспечения средств защиты информации;

– наличие проверок настройки правильности функционирования программного обеспечения и средств защиты информации в информационной системе персональных данных;

– организацию физического доступа к техническим средствам, средствам защиты информации информационной системы персональных данных (в том числе опечатывание корпуса средств вычислительной техники);

– организацию размещения технических средств отображения информации информационных систем персональных данных, исключая ее несанкционированный просмотр;

– состав технических средств, программного обеспечения и средств защиты информации, входящих в состав информационной системы на соответствие Техническому паспорту информационной системы в случае, если запланировано проведение работ по аттестации информационной системы персональных данных;

– реализацию процесса управления конфигурацией информационной системы персональных данных и системы защиты персональных данных в случае, если запланировано проведение работ по аттестации информационной системы персональных данных.

3.7.4. Проанализировать состояние работы в УУНиТ по реализации организационных и технических мер по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации, в соответствии с Постановлением Правительства РФ от 15.09.2008 № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" и проверить:

– обеспечение обособления персональных данных при их обработке, осуществляемой без использования средств автоматизации, от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных;

– контроль за недопущением копирования информации из журналов пропуска и иных документов;

– обеспечение раздельного хранения персональных данных, обрабатываемых в различных целях;

– наличие в типовых формах (например, согласия, заявления) всех реквизитов, предусмотренных п. 7 Постановления Правительства РФ от 15.09.2008 № 687.

4. Права комиссии по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

4.1. Комиссия при проведении проверки вправе:

– запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;

– получать в соответствии с Инструкцией пользователей информационной системы персональных данных временный доступ к ресурсам информационной системы персональных данных, в части касающейся ее полномочий;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;

– вносить ректору УУНиТ предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите персональных данных, установленных нормативными правовыми актами Российской Федерации.

4.2. При проведении проверки члены Комиссии не вправе:

– требовать представления документов и сведений, не относящихся к предмету проверки;

– распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

4.3. По результатам проверки составляется Акт проверки по форме Приложения к настоящим Правилам, который подписывается всем составом комиссии и представляется ректору УУНиТ для принятия соответствующего решения.

4.4. В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях обязательных требований законодательных и нормативных правовых актов Российской Федерации в области защиты персональных данных, об их характере и о лицах, допустивших указанные нарушения.

4.5. Акт должен содержать заключение о соответствии или несоответствии обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике УУНиТ в отношении обработки персональных данных, локальным нормативным актам УУНиТ.

4.6. Работники УУНиТ несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящими Правилами в соответствии с законодательством Российской Федерации.

Приложение
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных в УУНиТ

ФОРМА

Акт № _____
проведения внутренней проверки условий обработки персональных данных в УУНиТ

Дата составления: «____» _____ 20____ г.
Место проведение проверки: _____

Комиссия, назначенная приказом УУНиТ от «___» _____ 20___ № ____ в составе:
Председатель:
_____(Ф.И.О.)
Члены комиссии:
_____(Ф.И.О.)
_____(Ф.И.О.),
руководствуясь Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в УУНиТ, провела проверку условий обработки персональных данных в УУНиТ (оператор).
В ходе проверки:
- проведен анализ реализации мер, направленных на обеспечение выполнения оператором обязанностей, предусмотренных статьями 18.1, 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним локальными нормативными актами УУНиТ, определяющими его политику в отношении обработки персональных данных;
- проведен анализ выполнения оператором требований по определению и обеспечению уровня защищенности персональных данных при их обработке в информационной системе персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- проведен анализ реализации в УУНиТ организационных и технических мер по обеспечению безопасности персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- проведен анализ состава оборудования, программных средств, включая средства защиты, входящих в состав информационной системы персональных данных, на соответствие техническому паспорту информационной системы.

Выявленные нарушения: _____
_____
_____
_____

ЗАКЛЮЧЕНИЕ комиссии:
Обработка персональных данных соответствует / не соответствует *(нужное подчеркнуть)* Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным нормативным актам оператора.

Председатель комиссии _____ (подпись)
Члены комиссии: _____ (подпись)
_____ (подпись)
_____ (подпись)