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

ПРИКАЗ

16.10.2025 № 2889

Уфа

Об утверждении Положения о порядке организации и проведении работ по защите персональных данных, обрабатываемых в информационных системах 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 и ввести в действие с даты подписания настоящего приказа Положение о порядке организации и проведению работ по защите персональных данных, обрабатываемых в информационных системах персональных данных в ФГБОУ ВО «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.

3. Общему отделу (Рахимова Д.Ф.) обеспечить рассылку настоящего приказа проректорам и во все структурные подразделения УУНиТ, в том числе в филиалы.

4. Руководителям структурных подразделений, директорам филиалов УУНиТ ознакомить под подпись с настоящим приказом работников и обучающихся.

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: 16-10-2025 16:08:05
Действителен с 2024-9-9 12:33:19 по 2025-12-3 12:33:19

Приложение к приказу
от 16.10.2025 № 2889

Положение
о порядке организации и проведения работ по защите персональных данных, обрабатываемых в информационных системах персональных данных в ФГБОУ ВО «Уфимский университет науки и технологий»

1.Общие положения

1.1. Настоящее Положение о порядке организации и проведения работ по защите персональных данных, обрабатываемых в информационных системах персональных данных в ФГБОУ ВО «Уфимский университет науки и технологий» (далее – Положение) разработано в соответствии со следующими нормативными правовыми актами Российской Федерации в области обработки и защиты персональных данных:

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

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

приказ 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».

1.2. В настоящем Положении используются следующие сокращения и определения, применяемые законодательством Российской Федерации в области обработки и защиты персональных данных:

ПДн – персональные данные;

Роскомнадзор – уполномоченный орган по защите прав субъектов персональных данных;

ФСТЭК России – федеральная служба по техническому и экспортному контролю;

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 – Университет (УУНиТ);

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

Безопасность информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

ПО - программное обеспечение;

Антивирусное ПО – программное обеспечение средств антивирусной защиты;

Вредоносное ПО – вредоносная компьютерная программа (вирус);

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы;

Компьютерный вирус - вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы;

АРМ – автоматизированное рабочее место;

СВТ – средства вычислительной техники;

Администратор безопасности – работник, ответственный за обеспечение безопасности ПДн в информационной системе ПДн;

Администратор системный – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы в соответствии с установленными полномочиями;

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность;

Событие информационной безопасности – идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности, отказ защитных мер, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью;

Машинный носитель информации – материальный носитель, используемый для передачи и хранения защищаемой информации (в том числе ПДн) в электронном виде.

1.3. Администратор безопасности, администратор системный и пользователи информационных систем ПДн (далее – информационных систем) должны быть ознакомлены с настоящим положением до начала работы в информационных системах под подпись. Обязанность по организации ознакомления пользователей с настоящей Инструкцией возлагается на ответственного за организацию обработки ПДн и лиц, которым делегировано данное поручение.

1.4. Для координации и контроля выполнения мероприятий по организации обработки и защиты ПДн в Университете приказом назначается лицо, ответственное за организацию обработки персональных данных. При выполнении своих служебных (трудовых) обязанностей ответственный за организацию обработки ПДн руководствуется требованиями Инструкции ответственного за организацию обработки ПДн в УУНиТ.

В УУНиТ утверждены Правила обработки ПДн информационных систем персональных данных в целях:

- обеспечения защиты прав и свобод субъектов персональных данных при обработке ПДн в Университете;

- установления процедур, направленных на выявление и предотвращение нарушений законодательства Российской Федерации о ПДн, иных правовых актов Российской Федерации, внутренних документов УУНиТ по вопросам обработки и защиты ПДн;

- определения целей обработки ПДн в информационных системах в установленной сфере деятельности, включая содержание обрабатываемых ПДн, категории субъектов ПДн, данные которых обрабатываются, сроки обработки (в том числе хранения) обрабатываемых ПДн, а также порядок уничтожения ПДн при достижении целей обработки или при наступлении иных законных оснований;

- установления ответственности работников Университета, имеющих доступ к ПДн субъектов персональных данных в информационных системах, за невыполнение требований норм, регулирующих обработку ПДн, установленных законодательством Российской Федерации, настоящим Положением и иными локальными актами УУНиТ.

Для непосредственного выполнения работ по защите персональных данных с использованием программно-аппаратных средств защиты информации назначается лицо, ответственное за обеспечение безопасности персональных данных в информационных системах (далее – администратор безопасности)

При выполнении своих обязанностей администратор безопасности действует в соответствии с требованиями Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах ПДн в УУНиТ и требованиями

эксплуатационной документации на средства защиты информации, используемые в составе системы защиты информации.

Все пользователи информационных систем участвуют в защите персональных данных, содержащихся в информационных системах, и обязаны знать и выполнять требования:

- нормативных правовых документов Российской Федерации по защите информации, в том числе по защите персональных данных;
- настоящего Положения и перечисленных в нём инструкций, в части их касающейся;
- Инструкции пользователя информационных систем персональных данных в УУНиТ.

В ходе эксплуатации информационных систем персональных данных защита ПДн обеспечивается выполнением процедур:

управления (администрирования) системой защиты информации в информационных системах;

контроля обеспечения уровня защищённости ПДн в информационных системах.

2. Управление системой защиты ПДн информационных систем

2.1. Процедуры управления системой защиты ПДн обеспечивают:

- функционирование системы защиты ПДн информационных систем в штатном режиме с характеристиками, установленными в проектной документации;
- документированный поток информации о событиях безопасности в информационных системах и их системах защиты, на основании которой возможны реализация процедуры контроля уровня защищённости ПДн, обрабатываемых в информационных системах.

Порядок действий пользователей информационных систем при прохождении процедур идентификации (узнавания) и аутентификации (подтверждения подлинности узнанного пользователя) при входе в информационные системы описаны в Инструкции по идентификации и аутентификации пользователей информационных систем ПДн в УУНиТ.

Порядок управления доступом пользователей к информационным ресурсам информационных систем устанавливается в Инструкции по управлению доступом к информационным системам ПДн в УУНиТ.

Порядок действий пользователей информационных систем при работе с машинными носителями ПДн, правила учёта, хранения и доступа к машинным носителям описаны в Инструкции по защите машинных носителей ПДн в УУНиТ.

Порядок действий администратора безопасности и системных администраторов информационных систем при появлении событий безопасности описаны в Инструкции по управлению событиями информационной безопасности информационных систем ПДн в УУНиТ.

Порядок действий пользователей при обнаружении вредоносного ПО описан в Инструкции по антивирусной защите информационных систем ПДн в УУНиТ.

Порядок действий системных администраторов и администратора безопасности информационных систем с целью:

- выявления ошибок и недостатков программного обеспечения и аппаратных средств, и средств защиты ПДн информационных систем;
- контроля установки обновлений программного обеспечения, контроля работоспособности и настроек программного обеспечения;
- контроля состава технических и программных средств информационных систем, в том числе средств защиты информации, описан в Инструкции по контролю (анализу) защищенности ПДн информационных систем персональных данных в УУНиТ.

Порядок доступа пользователей к техническим средствам информационных систем, в том числе к техническим средствам системы защиты информации, описан в Инструкции по защите технических средств информационных систем ПДн в УУНиТ.

Организация резервного копирования и восстановления ПДн в информационных

системах осуществляется администратором безопасности с заданной периодичностью, определяемой Инструкцией по обеспечению доступности информации информационных систем ПДн в УУНиТ (при наличии).

Организация режима безопасности помещений, в которых размещены информационные системы, правила доступа в помещения в рабочее, нерабочее время и в нештатных ситуациях определены в Порядке доступа в помещения, в которых размещены информационные системы ПДн в УУНиТ.

Обеспечение безопасности ПДн при обработке в информационных системах с использованием средств криптографической защиты информации осуществляется в соответствии с Положением по использованию средств криптографической защиты информации в УУНиТ, Порядком доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств в УУНиТ, Инструкцией пользователя средств криптографической защиты информации в УУНиТ, Инструкцией ответственного пользователя средств криптографической защиты информации в УУНиТ.

3. Контроль обеспечения уровня защищённости персональных данных информационных систем

3.1. Периодичность контроля обеспечения уровня защищённости ПДн, обрабатываемых в информационных системах, составляет 1 год.

Для контроля обеспечения уровня защищённости используются следующие документы:

- отчёты о событиях информационной безопасности;
- результаты контроля защищённости;
- информация из специальных источников по новым угрозам безопасности для используемых в информационных системах программных и программно-технических средств.

На основе указанных выше документов ответственный за организацию обработки ПДн в УУНиТ проводит:

- анализ функционирования системы защиты информации, включая сбои и неисправности аппаратно-программных средств защиты информации;
- анализ изменения угроз безопасности ПДн, обрабатываемых в информационных системах.

К анализу привлекаются системные администраторы и администратор безопасности. По отдельному договору к анализу могут быть привлечены специалисты сторонних организаций.

3.2. Ответственный за организацию обработки ПДн в УУНиТ организует документирование результатов проведённого анализа в виде Акта контроля обеспечения защищённости ПДн (акт составляется в произвольной форме и подписывается ответственным за организацию обработки ПДн в УУНиТ и администратором безопасности).

На основании выводов Акта контроля защищённости ПДн ответственный за организацию обработки ПДн в УУНиТ при необходимости доработки системы защиты ПДн докладывает об этом ректору УУНиТ.

Решение о доработке и последующей аттестации принимает ректор УУНиТ.

4. Ответственность

4.1. Пользователи информационных систем должны быть предупреждены об ответственности за действия с ПДн, содержащимися в информационных системах, и действия с техническими средствами информационных систем.