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

ПРИКАЗ

15.10.2025 № 2861

Уфа

О назначении ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в УУНиТ и утверждении Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в УУНиТ

В целях исполнения требований Федерального закона от 27.07.2006 № 152- ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», п р и к а з ы в а ю:

1. Назначить Галиева С. Р., начальника отдела защиты информации ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных в УУНиТ (далее также администратор безопасности).
2. Утвердить Инструкцию ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в УУНиТ (приложение).
3. Галиеву С. Р. при обеспечении безопасности персональных данных в информационных системах персональных данных в УУНиТ руководствоваться приложенной к настоящему приказу инструкцией.
4. Управлению персонала (Койда Л. А.) ознакомить администратора безопасности начальника отдела защиты информации Галиева С. Р. с настоящим приказом под подпись, а также обеспечить внесение соответствующих изменений в должностную инструкцию начальника отдела защиты информации.
5. Руководителям структурных подразделений, директорам филиалов, институтов довести содержание настоящего приказа до сведения работников.
6. 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.
7. Общему отделу (Рахимова Д.Ф.) обеспечить рассылку настоящего приказа проректорам и во все структурные подразделения УУНиТ, в том числе в филиалы.
8. 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: 15-10-2025 18:12:45
Действителен с 2024-9-9 12:33:19 по 2025-12-3 12:33:19

Приложение к приказу
от 15.10.2025 № 2861

**Инструкция ответственного
за обеспечение безопасности персональных данных в информационных системах персональных данных в УУНиТ**

1. Общие положения

1.1. Инструкция ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее - Инструкция) определяет в УУНиТ обязанности и права работника, назначенного ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных в УУНиТ (далее - администратор безопасности).

1.1. В своей деятельности администратор безопасности руководствуется законодательством Российской Федерации, иными нормативными правовыми актами Российской Федерации в сфере обработки и защиты персональных данных, локальными актами УУНиТ, а также настоящей Инструкцией.

1.2. Администратор безопасности назначается приказом УУНиТ и обеспечивает в пределах своих трудовых (служебных) обязанностей безопасность персональных данных, обрабатываемых в информационных системах персональных данных (далее – ИСПДн) в УУНиТ.

2. Обязанности администратора безопасности

2.1 Администратор безопасности при эксплуатации ИСПДн обязан:

−соблюдать требования законодательных и нормативных документов по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн.

−выполнять и принимать меры к выполнению требований организационно-распорядительной документации по организации обработки и защиты персональных данных в ИСПДн.

2.2 Осуществлять установку, настройку и сопровождение технических средств защиты ИСПДн;

2.3 Осуществлять организационное и техническое обеспечение процессов создания, использования, изменения и прекращения действия персональных идентификаторов и паролей доступа в ИСПДн;

2.4 Осуществлять контроль действий пользователей ИСПДн при их работе с персональными идентификаторами и паролями доступа:

−создавать, присваивать, уничтожать персональные идентификаторы и пароли доступа к техническим средствам и информационным ресурсам ИСПДн;

−хранить, выдавать, инициализировать, блокировать средства аутентификации (пароли, аппаратные идентификаторы) и принимать меры в случае утраты или компрометации средств аутентификации;

−вести, надежно хранить и в установленном порядке уничтожать Журналы учета выдачи первичных паролей информационных систем персональных данных;

−надежно хранить и вести учет аппаратных средств аутентификации по Журналу учета аппаратных средств аутентификации УУНиТ;

−надежно хранить и в установленном порядке уничтожать Журнал учета аппаратных средств аутентификации УУНиТ;

−обеспечивать смену паролей пользователей с периодичностью не реже одного раза в 90 дней с момента очередной смены и изменять свой собственный пароль не реже 1 раза в месяц. Принимать меры по обеспечению внеплановой смены паролей в случае их компрометации или утере индивидуальных аппаратных идентификаторов;

−сообщать ответственному за организацию обработки персональных данных в УУНиТ

об инцидентах, связанных с компрометацией или утерей паролей, аппаратных идентификаторов;

–выявлять и пресекать действия пользователей, которые могут привести к компрометации паролей и (или) утрате аппаратных идентификаторов.

2.5. Осуществлять и контролировать разграничение доступа пользователей к ресурсам и персональным данным, обрабатываемым в ИСПДн, путем настройки программно-технических средств и средств защиты информации:

–управлять учетными записями (заведение, активацию, блокирование, уничтожение), в том числе осуществлять блокирование учетной записи при превышении времени неиспользования более 90 дней, в случае достижения установленного максимального количества неуспешных попыток аутентификации в течение не более 30 минут (максимальное количество неуспешных попыток аутентификации до блокировки до 5 попыток), блокирование сеанса доступа в ИСПДн после установленного времени бездействия (неактивности) пользователя 30 минут или по его запросу;

–обеспечивать актуальность, сохранность и конфиденциальность матриц доступа к ресурсам ИСПДн, утвержденных приказом УУНиТ;

–вести учет технических средств удаленного доступа (в случае использования удаленного доступа через сеть Интернет к ресурсам ИСПДн) с документальным оформлением в Журнале учета разрешенных средств удаленного доступа в УУНиТ, а также осуществлять выдачу, хранение технических средств удаленного доступа, установку и настройку программного обеспечения, его обновление, антивирусную защиту технических средств удаленного доступа и контролировать использование технических средств удаленного доступа к ИСПДн;

–вести учет мобильных технических средств (в случае использования мобильных технических средств для доступа к ресурсам ИСПДн) с документальным оформлением в Журнале учета разрешенных мобильных технических средств в УУНиТ и контролировать использование мобильных технических средств для доступа к ИСПДн.

2.6. Вести учет, хранение и выдачу машинных носителей персональных данных, в том числе:

–организовывать и контролировать процедуру уничтожения (стирания) или обезличивания персональных данных при передаче между пользователями, в сторонние организации для ремонта или утилизации, а также факт уничтожения машинного носителя персональных данных;

–участвовать в составе комиссии по проверке наличия и состояния машинных носителей персональных данных;

–в случае выхода из строя, порчи или утраты машинного носителя персональных данных докладывать об инциденте ответственному за организацию обработки персональных данных в УУНиТ.

2.7. Контролировать проведение резервного копирования технических средств ИСПДн (при организации).

2.8. Осуществлять настройку журналов регистрации событий информационной безопасности в программном обеспечении ИСПДн и средств защиты информации в части касающейся, фиксировать информацию о событиях безопасности в информационных системах, не подлежащую автоматической регистрации в Журнале событий информационной безопасности информационной системы персональных данных.

Вести, надежно хранить Журнал событий информационной безопасности информационной системы персональных данных.

2.9. Осуществлять установку, конфигурирование и управление средствами антивирусной защиты ИСПДн, в том числе:

–установку и обновление лицензионных ключей средств антивирусной защиты, обновлений базы признаков вредоносных компьютерных программ (вирусов);

−принимать меры по локализации и удалению вредоносного программного обеспечения, выявлению источника и способа проникновения вредоносного программного обеспечения;

−восстановление работоспособности программных средств и информационных массивов программных средств, поврежденных вредоносным программным обеспечением;

−ограничение доступа пользователей на автоматизированным рабочих местах (далее - АРМ) к настройкам установленных средств антивирусной защиты;

− контроль над работой пользователей ИСПДн по применению на непосредственных АРМ средств антивирусной защиты,

−немедленно оповещать ответственного за организацию обработки персональных данных в УУНиТ об обнаружении вредоносного программного обеспечения на серверном или телекоммуникационном оборудовании.

2.10. Осуществлять исполнение мероприятий по выявлению (поиску), анализу и устранению уязвимостей в ИСПДн (с разработкой Плана устранения выявленных уязвимостей):

−осуществлять мониторинг наличия обновлений, выпускаемых разработчиками программного обеспечения, используемого в ИСПДн и средствах защиты информации, в части касающейся;

−проводить обновление программного обеспечения средств защиты информации, программного обеспечения программно-аппаратных средств в случае выявления уязвимостей, связанных с устаревшими версиями программного обеспечения;

−выполнять необходимые настройки, проводить тестирование работоспособности после установки обновлений программного обеспечения и вносить необходимые изменения в эксплуатационную документацию;

−проводить контроль установки обновлений программного обеспечения (проводить проверку соответствия версии общесистемного, прикладного и специального программного обеспечения, установленного в ИСПДн, а также программного обеспечения средств защиты информации, выпущенного разработчиком, наличия соответствующих отметок в Техническом паспорте и в эксплуатационной документации);

−не реже 1 раза в полгода проводить контроль на соответствие Техническим паспортам ИСПДн состава технических средств, программного обеспечения и средств защиты информации.

−осуществлять проверку наличия и сроков действия лицензий на установленное программное обеспечение ИСПДн и программное обеспечение средств защиты информации, сертификатов соответствия на примененные в ИСПДн и средствах защиты информации программно-аппаратных средств;

−ежемесячно проводить контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;

−немедленно уведомлять ответственного за организацию обработки персональных данных в УУНиТ при получении информации о прекращении поддержки разработчиком используемого программного обеспечения в части выпуска обновлений безопасности, либо о планируемом прекращении такой поддержки;

−проводить проверку технического состояния аппаратных средств, журналов планово-профилактического обслуживания аппаратных средств ИСПДн за период контроля защищенности ИСПДн, перечня событий информационной безопасности за период контроля, связанных с отказами и неисправностями аппаратных средств, конфигурацию соединений и установки аппаратных средств, условия их эксплуатации;

−осуществлять контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации, в случае

выявления сбоев, отказов или несоответствия настройкам, организовывать восстановление программного обеспечения и средств защиты информации;

–участвовать в организованной ответственным за организацию обработки персональных данных в УУНиТ проверке состояния и актуальности организационно-распорядительной документации по защите персональных данных, обрабатываемых в ИСПДн.

2.11. Проводить анализ планируемых изменений в конфигурацию ИСПДн и системы защиты персональных данных, отнесенным к 3 уровню защищенности персональных данных при их обработке в ИСПДн, и принимать решение о необходимости внесения изменения в конфигурацию ИСПДн и системы защиты персональных данных, осуществлять проверку корректности изменения конфигурации и при необходимости совместно с ответственным за организацию обработки персональных данных в УУНиТ организовать актуализацию документации по вопросам обеспечения безопасности персональных данных при их обработке в ИСПДн, а также контроль эффективности обеспечения безопасности персональных данных при их обработке в ИСПДн.

2.12. Контролировать выполнение требований к размещению устройств вывода информации в контролируемых зонах, расположение технических устройств и физический доступ к ним.

3. Права администратора безопасности

3.1. Администратор безопасности имеет право:

– привлекать к работам, связанным с обеспечением безопасности персональных данных в ИСПДн системных администраторов ИСПДн;

– требовать от пользователей ИСПДн выполнения установленной технологии обработки информации, инструкций по обеспечению информационной безопасности ИСПДн;

– докладывать ответственному за организацию обработки персональных данных в УУНИТ о нарушениях или невыполнении пользователями требований обеспечению безопасности персональных данных;

– вносить предложения по модернизации и совершенствованию систем защиты персональных данных в УУНиТ ответственному за организацию обработки персональных данных в УУНиТ;

– останавливать обработку персональных данных в ИСПДн в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования средств защиты информации.

4. Ответственность

Администратор безопасности несет ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей Инструкцией, в соответствии с действующим законодательством Российской Федерации.

ЛИСТ ОЗНАКОМЛЕНИЯ

с приказом УУНиТ от «___» _____ 2025 года № ____ «О назначении ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в УУНиТ и утверждении Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных в УУНиТ»

№ п/п	ФИО	Должность	Дата	Подпись