

Министерство сельского хозяйства Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уральский государственный аграрный университет»
(ФГБОУ ВО Уральский ГАУ)

ПРИКАЗ

«30» августа 2024 г.

№ 422

г. Екатеринбург

О внутреннем контроле в области
защиты персональных данных

Руководствуясь Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также в соответствии с пунктом 3.2 приказа ФГБОУ ВО Уральский ГАУ от 26 июня 2024 г. № 323 «О безопасности персональных данных»

П Р И К А З Ы В А Ю:

1. Создать комиссию по организации обработки и защите персональных данных в ФГБОУ ВО Уральский ГАУ и утвердить:

состав комиссии по организации обработки и защите персональных данных в ФГБОУ ВО Уральский ГАУ (приложение № 1);

Положение о комиссии по организации обработки и защите персональных данных в ФГБОУ ВО Уральский ГАУ (приложение № 2).

2. Проректорам, главному бухгалтеру, директору института, деканам факультетов, руководителям иных структурных подразделений ФГБОУ ВО Уральский ГАУ довести настоящий приказ до сведения подчиненных работников.

3. Приказ от 1 ноября 2022 г. № 511 «О создании комиссии по защите персональных данных и организации мероприятий по контролю за обеспечением безопасности персональных данных в ФГБОУ ВО Уральский ГАУ» считать утратившим силу.

4. Контроль исполнения настоящего приказа возлагаю на проректора по правовым вопросам и имущественным отношениям А.В. Портнягина.

Ректор

О.Г. Лоретц

Состав
комиссии по организации обработки и защите персональных данных
в ФГБОУ ВО Уральский ГАУ

№	Состав комиссии	Должность, фамилия, имя, отчество
1	Председатель комиссии	Проректор по правовым вопросам и имущественным отношениям А.В. Портнягин
2	Заместитель председателя комиссии	Начальник управления безопасности А.С. Сысун
3	Заместитель председателя комиссии	Начальник управления информационных технологий А.Н. Путилов
4	Секретарь комиссии	Главный специалист по информационной безопасности управления безопасности П.П. Усков
5	Член комиссии	Начальник правового управления К.А. Попова
6	Член комиссии	Заместитель начальника департамента кадровой политики С.В. Петрякова

Положение
о комиссии по организации обработки и защите персональных данных
в ФГБОУ ВО Уральский ГАУ (далее – комиссия)

1. Общие положения

1.1. Настоящее Положение о комиссии по организации обработки и защите персональных данных в ФГБОУ ВО Уральский ГАУ (далее – Положение) определяет процедуры, направленные на предотвращение нарушений законодательства Российской Федерации в сфере защиты персональных данных, в том числе основания и порядок осуществления внутреннего контроля соответствия обработки персональных данных субъектов персональных данных требованиям к защите персональных данных (далее – внутренний контроль).

1.2. Целью Положения является обеспечение защиты персональных данных от несанкционированного доступа, неправомерного их использования или утраты.

1.3. Положение разработано на основании Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», 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», приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Для обработки персональных данных в ФГБОУ ВО Уральский ГАУ (далее – университет) используются информационные системы персональных данных, перечень которых утверждается ректором университета.

2. Основные функции комиссии

2.1. Комиссия осуществляет внутренний контроль путем:

подготовки и актуализации локальных нормативных актов по вопросам организации сбора, учета, обработки, порядка хранения, передачи и защиты персональных данных;

проведения проверок соблюдения правил доступа к персональным данным субъектов персональных данных, условий применения средств защиты информации, состояния учета съемных носителей информации, содержащих персональные данные, состояния учета машинописных носителей персональных данных;

проведения служебных проверок по фактам несанкционированного доступа к персональным данным и принятия мер по пресечению таких фактов;

применения иных правовых, технических и организационных мер по обеспечению безопасности персональных данных.

3. Основные задачи комиссии

3.1. Основными задачами комиссии являются:

оценка эффективности правовых, технических и организационных мер, принимаемых для защиты персональных данных;

выявление и анализ нарушений требований к защите персональных данных, принятие мер по пресечению выявленных нарушений, а также устранение их причин и условий;

обеспечение мер по устранению недостатков, выявленных в результате проведения внутреннего контроля;

организация приема и рассмотрения обращений и запросов субъектов персональных данных или их законных представителей о реализации прав и законных интересов при обработке персональных данных;

доведение до работников университета требований законодательства Российской Федерации, локальных нормативных актов и рекомендаций по организации сбора, обработки, хранения, передачи и защиты персональных данных.

3. Полномочия комиссии

3.1. Комиссия имеет право:

запрашивать и знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на комиссию задач;

принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации, в том числе требовать от работников университета, уполномоченных на обработку персональных данных, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

инициировать и проводить служебные проверки по выявленным фактам нарушения требований законодательства Российской Федерации в области защиты персональных данных;

вносить по результатам внутреннего контроля и служебных проверок предложения о привлечении к дисциплинарной ответственности работников университета, виновных в нарушении законодательства Российской Федерации в области защиты персональных данных;

вносить предложения о совершенствовании правового, технического и организационного обеспечения безопасности персональных данных.

3.2. В осуществлении внутреннего контроля, в том числе в проведении служебных проверок по выявленным нарушениям не может участвовать работник университета, заинтересованный в ее результатах.

3.3. Члены комиссии, получившие доступ к персональным данным субъектов персональных данных в ходе проведения проверки, обеспечивают конфиденциальность персональных данных, не раскрывают третьим лицам и не распространяют персональные данные без согласия субъекта персональных данных.

4. Состав и порядок работы комиссии

4.1. В состав комиссии входят председатель комиссии, заместители председателя комиссии, секретарь комиссии и члены комиссии, определенные приказом ректора университета.

4.2. Председатель комиссии:

осуществляет общее руководство деятельностью комиссии, организует работу комиссии;

проводит заседания комиссии по мере необходимости;

осуществляет общий контроль за реализацией принятых комиссией решений.

4.3. Заместители председателя комиссии:

выполняют поручения председателя комиссии по планированию, подготовке, организации и проведению проверок соблюдения обязательных требований законодательства Российской Федерации в области защиты персональных данных;

выполняют обязанности председателя комиссии в его отсутствие.

4.4. Секретарь комиссии:

доводит до сведения членов комиссии повестку дня заседания комиссии и направляет членам комиссии материалы, связанные с ее деятельностью;

информирует членов комиссии о дате, времени и месте проведения заседаний комиссии;

осуществляет организационные мероприятия, связанные с подготовкой заседаний комиссии, включая прием и рассмотрение документов, предоставляемых членами комиссии к ее заседаниям;

оформляет протоколы заседаний комиссии;

решает иные вопросы, связанные с деятельностью комиссии, по поручению председателя комиссии или его заместителей в отсутствие председателя комиссии.

4.5. Члены комиссии:

участвуют в заседаниях Комиссии;

осуществляют внутренний контроль;

участвуют в проведении служебных проверок и реализации иных задач комиссии.

4.6. Заседание комиссии считается правомочным, если на нем присутствует не менее половины общего числа ее членов.

4.7. Решения комиссии принимаются простым большинством голосов присутствующих на заседании членов Комиссии. При равенстве голосов членов комиссии решающим является голос председателя комиссии, а в случае его отсутствия – заместителя, председательствующего на заседании комиссии.

4.8. Заседания комиссии проводятся по мере необходимости.

4.9. Ежегодный отчет о результатах работы комиссии докладывается ректору университета.

Ежегодный отчет должен содержать:

оценку текущего состояния правовых, организационных, инженерно-технических (технических и программных) мероприятий по обеспечению защиты персональных данных;

оценку существующего порядка и результатов принятых мер по совершенствованию защиты персональных данных;

оценку выполнения обязательных требований по обеспечению защиты персональных данных (с учетом результатов внутреннего контроля);

общие выводы об уровне защищенности персональных данных относительно допустимого уровня риска;

основания проведенных в рамках внутреннего контроля проверок, виды проверок (плановые и внеплановые), цель их проведения, выявленные нарушения, принятые меры;

рекомендации по осуществлению дополнительного комплекса мер правового, технического и организационного характера, направленных на выявление и ликвидацию различных видов угроз и организацию эффективно функционирующей системы защиты персональных данных;

рекомендации по разработке аналитического обоснования создания (модернизации) системы (подсистемы) защиты персональных данных.

4.10. Протоколы заседаний комиссии и ежегодные отчеты о результатах работы комиссии хранятся у секретаря комиссии.

5. Порядок осуществления внутреннего контроля

5.1. Внутренний контроль осуществляется в целях изучения и оценки фактического состояния защищенности персональных данных, своевременного реагирования на нарушения установленного порядка их обработки, хранения и передачи, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

5.2. Внутренний контроль включает:

контроль ознакомления работников, осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к их защите, а также локальными нормативными актами в указанной области;

оценку актуальности локальных нормативных актов по вопросам обработки и защиты персональных данных;

оценку эффективности применения правовых, организационных и технических мер по обеспечению безопасности персональных данных;

включение в положения о структурных подразделениях университета и должностные инструкции работников университета обязанностей и ответственности в области обработки и защиты персональных данных;

осуществление мероприятий по обеспечению целостности персональных данных;

обеспечение соблюдения правил доступа к персональным данным;

проверка наличия (отсутствия) фактов несанкционированного доступа к персональным данным, принятие необходимых мер;

проверка соблюдения пользователями информационных систем персональных данных локальных нормативных актов университета по вопросам обработки персональных данных;

соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных;

обеспечение условий хранения материальных носителей персональных данных (допускается только в помещениях или шкафах, оборудованных надежными замками и другими необходимыми средствами защиты от несанкционированного проникновения);

соблюдение порядка работы со средствами защиты информации;

выполнение работниками правил работы с атрибутами доступа к персональным данным (не передавать другим лицам, исключить возможность просмотра, не хранить на бумажных или электронных носителях в открытом (незашифрованном) виде);

соблюдение порядка хранения бумажных носителей с персональными данными;

осуществление доступа к бумажным носителям с персональными данными;

выявление нарушений установленного порядка обработки персональных данных, своевременное предотвращение негативных последствий таких нарушений;

принятие мер, направленных на устранение выявленных нарушений порядка обработки персональных данных и в работе технических средств информационных систем персональных данных, их причин и условий;

разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных по результатам внутреннего контроля;

иные мероприятия по решению председателя комиссии.

5.3. В целях осуществления внутреннего контроля комиссией организуется проведение плановых и (или) внеплановых проверок по вопросам соблюдения требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

5.4. Проверки проводятся на основании ежегодного плана и (или) на основании поступившей информации о нарушении правил обработки персональных данных (внеплановые проверки).

5.5. Ежегодный план проверок утверждается ректором университета.

В ежегодном плане проверок по каждой проверке устанавливается объект внутреннего контроля, проверяемый период, срок проведения проверки, ответственные исполнители.

5.6. Основаниями для проведения внеплановой проверки являются:

письменное обращение субъекта персональных данных или его представителя о нарушении правил обработки, хранения и передачи персональных данных;

обращения органов государственной власти по вопросам защиты персональных данных.

5.7. Проведение внеплановой проверки организуется в течении 5 рабочих дней со дня поступления соответствующего обращения или в срок, установленный в обращении органа государственной власти.

5.8. Срок проведения проверки не может превышать 20 дней со дня принятия решения об ее проведении.

5.9. Проверки проводятся непосредственно на месте обработки персональных данных путем опроса работников, участвующих в процессе обработки, хранения и передачи персональных данных, либо путем осмотра их рабочих мест.

5.10. В случаях выявления нарушений обработки, хранения и передачи персональных данных, требующих немедленного устранения, комиссией принимаются меры оперативного реагирования, направленные на предотвращение негативных последствий выявленных нарушений.

5.11. Результаты внутреннего контроля:

оформляются актами плановых и внеплановых проверок, заключениями служебных проверок, протоколами заседаний комиссии с указанием конкретных мер по устранению нарушений, их причин и условий, а также ответственных лиц и сроков выполнения принятых комиссией решений;

являются основанием для разработки дополнительных рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных, модернизации технических средств информационных систем персональных данных и средств защиты персональных данных, по повышению квалификации работников, уполномоченных на обработку персональных данных.

5.12. Результаты проверок фиксируются в журнале (приложение № 1).

5.13. Выявленные нарушения фиксируются в журнале (приложение № 2).

