



МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Уральский государственный горный университет»

Стандарт организации

**Политика в отношении обработки персональных данных в
ФГБОУ ВО «Уральский государственный горный университет»**

СМК СТО 04-03.535-2025

Стр. 1 из 15

УТВЕРЖДАЮ

И. о. ректора ФГБОУ ВО «УГГУ»

_____ Г. И. Батрак

«20» июня 2025 г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

СТАНДАРТ ОРГАНИЗАЦИИ

**Политика в отношении обработки персональных данных
в ФГБОУ ВО «Уральский государственный горный университет»**

СМК СТО 04-03.535-2025

Версия 3.0

Дата введения: «20» июня 2025 г.

Екатеринбург – 2025

Версия:3.0

Дата утверждения версии 2.0:

31.12.2015



Содержание документа

1. Общие положения	3
2. Нормативные документы	3
3. Назначение Политики	3
4. Цели и задачи Политики. Принципы обработки персональных данных в УГГУ 4	
5. Условия и порядок обработки персональных данных в УГГУ	6
6. Основные принципы построения системы безопасности персональных данных 7	
7. Меры и методы обеспечения требуемого уровня защиты информационных ресурсов	10
8. Средства обеспечения безопасности персональных данных	11
9. Ответственность за нарушения в области обработки и защиты персональных данных	12
10. Утверждение, введение в действие и изменение Политики	13
11. Рассылка	13
Лист согласования	14
Регистрация изменений, дополнений и ревизий документов	15



1 Общие положения

Настоящая Политика в отношении обработки персональных данных (далее – Политика) в федеральном государственном бюджетном образовательном учреждении высшего образования «Уральский государственный горный университет» (далее – ФГБОУ ВО «УГГУ», УГГУ) определяет основные подходы и требования к обработке и защите персональных данных в УГГУ. Политика представляет собой систематизированное изложение целей, задач, принципов и условий обработки персональных данных и действует в отношении любой информации о субъекте персональных данных (физическом лице), которую УГГУ вправе обрабатывать.

2 Нормативные документы

Настоящая Политика разработана в соответствии с:

- Конституцией Российской Федерации;
- Трудовым кодексом Российской Федерации;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Уставом ФГБОУ ВО «УГГУ»;
- Положением о защите персональных данных работников и обучающихся федерального государственного бюджетного образовательного учреждения высшего образования «Уральский государственный горный университет», утвержденного ректором УГГУ 23 января 2025 г.

3 Назначение Политики

Политика является методологической основой для:

- принятия управленческих решений и разработки практических мер по воплощению политики в отношении обработки персональных данных и их защиты и выработки комплекса согласованных правовых, организационных, технических и иных мер, направленных на выявление угроз в отношении персональных данных и их ликвидацию (уменьшение) в УГГУ;
- координации деятельности структурных подразделений УГГУ при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации, которые применяются при обработке персональных данных;
- разработки предложений по совершенствованию правовых, организационных, технических и иных мер по обработке и защите персональных



данных в УГГУ;

– построения комплексной системы обработки и защиты персональных данных, в том числе при их обработке в информационных системах персональных данных УГГУ и должна способствовать оптимизации затрат на ее построение.

Действие настоящей Политики распространяется на персональные данные всех категорий субъектов персональных данных, обработка которых осуществляется в УГГУ, а именно:

- работников, состоящих в трудовых отношениях с УГГУ;
- абитуриентов, участвующих в конкурсе на зачисление в УГГУ;
- слушателей, студентов, аспирантов, докторантов, соискателей (далее – обучающихся);
- членов диссертационных советов, членов экзаменационных (государственных экзаменационных) комиссий;
- авторов охраняемых результатов интеллектуальной деятельности и средств индивидуализации;
- исполнителей по гражданско-правовым договорам, авторским договорам;
- посетителей УГГУ;
- физических лиц, пользующихся услугами УГГУ;
- физических лиц, вступающих в расчетно-финансовые отношения с УГГУ
- иных физических лиц, которые обращаются с запросами в УГГУ.

4 Цели и задачи Политики. Принципы обработки персональных данных в УГГУ

4.1 Основные цели Политики:

- повышение доверия к УГГУ со стороны абитуриентов, обучающихся, работников УГГУ и иных лиц;
- обеспечение режима конфиденциальности персональных данных, защиты от несанкционированного распространения;
- повышение стабильности функционирования УГГУ, а также обеспечение реализации уставных целей и осуществления направлений деятельности, указанных в Уставе УГГУ;
- содействие субъектам персональных данных в осуществлении учебной, научной, трудовой и иной деятельности, обеспечение защиты прав и свобод субъектов персональных данных УГГУ при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- регулирование отношений, связанных с обработкой персональных данных субъектов персональных данных, осуществляемой УГГУ;



- определение задач, принципов, условий и порядка обработки персональных данных субъектов персональных данных в УГГУ;
- обеспечение защиты прав и свобод субъектов персональных данных при обработке их персональных данных от несанкционированного доступа к ним;
- установление ответственности должностных лиц УГГУ за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

4.2 Основные задачи Политики:

- определение направлений деятельности УГГУ по обработке и защите персональных данных абитуриентов, обучающихся, работников УГГУ и иных лиц;
- установление оптимальных требований по обеспечению защиты персональных данных при их обработке с использованием средств автоматизации и без использования средств автоматизации;
- повышение эффективности мероприятий обработки и защиты персональных данных.

4.3 Принципы обработки персональных данных в УГГУ:

- обработка персональных данных в УГГУ должна осуществляться в соответствии с действующим законодательством в сфере защиты персональных данных, Уставом УГГУ, настоящей Политикой, Положением об обработке и защите персональных данных в УГГУ и иными локальными нормативными актами УГГУ;
- обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональных данных, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональных данных, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;
- при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- УГГУ должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных, или неточных данных;
- хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом и (или) договором, стороной которого

	ФГБОУ ВО «Уральский государственный горный университет»	
	СТО «Политика в отношении обработки персональных данных в ФГБОУ ВО «Уральский государственный горный университет»	
	СМК СТО 04-03.535-2025	Стр. 6 из 15

либо выгодоприобретателем, по которому является субъект персональных данных;

- обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5 Условия и порядок обработки персональных данных в УГГУ

5.1 Обработка персональных данных в УГГУ осуществляется с соблюдением принципов, определенных в статье 5 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

5.2 Обработка персональных данных допускается в следующих случаях:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных, за исключением случаев, определенных федеральными законами;

- обработка персональных данных необходима для осуществления и выполнения функций, полномочий и обязанностей, возложенных на УГГУ законодательством Российской Федерации, Уставом УГГУ и (или) договором;

- обработка персональных данных необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем;

- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

- обработка персональных данных необходима для осуществления прав и законных интересов УГГУ или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

- обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», при условии обязательного обезличивания персональных данных;

- осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных, либо по его

	ФГБОУ ВО «Уральский государственный горный университет»	
	СТО «Политика в отношении обработки персональных данных в ФГБОУ ВО «Уральский государственный горный университет»	
	СМК СТО 04-03.535-2025	Стр. 7 из 15

просьбе;

– осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами.

5.3 Обработка специальных категорий персональных данных, а также биометрических персональных данных в УГГУ осуществляется с учетом требований, установленных статьями 10 и 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

5.4 УГГУ вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключенного с этим лицом договора.

5.5 УГГУ осуществляет обработку персональных данных с использованием средств автоматизации и без использования средств автоматизации.

6 Основные принципы построения системы безопасности персональных данных

6.1 Законность. Предполагает осуществление защитных мероприятий и разработку системы безопасности персональных данных УГГУ в соответствии с действующим законодательством в области защиты персональных данных, а также других законодательных актов по безопасности информации Российской Федерации, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с персональными данными. Принятые меры безопасности персональных данных не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях. Все пользователи информационных систем персональных данных УГГУ должны иметь представление об ответственности за правонарушения в области обработки персональных данных.

6.2 Системность. Предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности персональных данных. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем персональных данных УГГУ, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников). Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.



6.3 Комплексность. Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

6.4 Непрерывность защиты. Для эффективного выполнения функций физических и технических средств защиты необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления защиты.

6.5 Своевременность. Предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите персональных данных и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационных систем персональных данных в целом и их систем защиты, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы персональных данных. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

6.6 Преемственность и совершенствование. Предполагает постоянное совершенствование мер и средств защиты персональных данных на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы персональных данных УГГУ и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

6.7 Разумная достаточность. Предполагает соответствие уровня затрат на обеспечение безопасности персональных данных ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационной системы персональных данных УГГУ. Излишние меры безопасности не должны приводить к экономической неэффективности, снижению эффективности работы персонала.



6.8 Персональная ответственность. Предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого работника в пределах его должностных обязанностей. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

6.9 Минимизация полномочий. Предполагает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к персональным данным должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

6.10 Исключение конфликта интересов. Предполагает четкое разделение обязанностей работников и исключение ситуаций, когда сфера ответственности работников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться и находиться под строгим независимым контролем.

6.11 Гибкость системы защиты. Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления УГГУ своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры УГГУ;
- изменение существующих или внедрение принципиально новых информационных систем персональных данных;
- новые технические средства и технологии.

6.12 Открытость алгоритмов и механизмов защиты. Защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже разработчикам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

6.13 Простота применения средств защиты. Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудовых затрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

6.14 Обоснованность и техническая реализуемость. Информационные технологии, технические и программные средства, средства и меры защиты персональных данных должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны

	ФГБОУ ВО «Уральский государственный горный университет»	
	СТО «Политика в отношении обработки персональных данных в ФГБОУ ВО «Уральский государственный горный университет»	
	СМК СТО 04-03.535-2025	Стр. 10 из 15

соответствовать установленным нормам и требованиям по безопасности персональных данных.

6.15 Специализация и профессионализм. Реализация административных мер и эксплуатация средств защиты должны осуществляться профессионально подготовленными специалистами УГГУ (ответственными за организацию обработки и защиты персональных данных).

6.16 Обязательность контроля. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности персональных данных на основе используемых систем и средств защиты персональных данных, при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Меры и методы обеспечения требуемого уровня защиты информационных ресурсов

7.1 При обработке персональных данных УГГУ должны приниматься необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

7.2 Обеспечение безопасности персональных данных, обрабатываемых в УГГУ, должно достигаться:

- назначением ответственных лиц за организацию обработки и обеспечение безопасности персональных данных в каждом подразделении УГГУ;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов УГГУ по вопросам обеспечения безопасности информации;
- подготовкой должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности персональных данных и процессов их обработки;
- персональной ответственностью за свои действия каждого работника, в рамках своих должностных обязанностей, имеющего доступ к информационным ресурсам УГГУ;
- осуществлением внутреннего контроля и/или аудита соответствия обработки персональных данных в УГГУ Федеральному закону от 27 июля 2006 года № 152-ФЗ

	ФГБОУ ВО «Уральский государственный горный университет»	
	СТО «Политика в отношении обработки персональных данных в ФГБОУ ВО «Уральский государственный горный университет»	
	СМК СТО 04-03.535-2025	Стр. 11 из 15

«О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, локальным актам УГГУ не реже 1 раза в три года;

- ознакомлением абитуриентов, обучающихся, работников УГГУ, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами УГГУ в отношении обработки персональных данных и/или обучением указанных работников;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных в УГГУ;

- выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер по их защите;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

7.3 При обработке персональных данных в информационных системах персональных данных необходимый уровень защиты должен достигаться:

- строгим учетом всех подлежащих защите ресурсов информационных систем персональных данных УГГУ (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

- наделением каждого работника (пользователя) минимально необходимыми для выполнения им своих должностных обязанностей полномочиями по доступу к информационным ресурсам УГГУ;

- четким знанием и строгим соблюдением всеми пользователями информационных систем персональных данных УГГУ требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных УГГУ;

- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды УГГУ;

- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования.

Средства обеспечения безопасности персональных данных

8.1 На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или

	ФГБОУ ВО «Уральский государственный горный университет»	
	СТО «Политика в отношении обработки персональных данных в ФГБОУ ВО «Уральский государственный горный университет»	
	СМК СТО 04-03.535-2025	Стр. 12 из 15

специальных аппаратных средств;

- регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информацией, находящейся на нем.

8.2 В состав системы защиты должны быть включены следующие технические средства защиты:

- средства разграничения доступа к данным;
- средства регистрации доступа к компонентам информационных систем персональных данных и контроля за использованием информации;
- средства реагирования на нарушения режима информационной безопасности.

8.3 Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа на контролируемую территорию, в отдельные помещения, к компонентам информационной среды УГГУ и элементам системы защиты персональных данных (физический доступ), к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.), к активным ресурсам (прикладным программам, задачам и т.п.), к операционной системе, системным программам и программам защиты.

8.4 Средства обеспечения целостности должны включать средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

8.5 Средства оперативного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток несанкционированного доступа и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций.

8.6 Для своевременного выявления и предотвращения утечки персональных данных за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение персональных данных, разрушение средств информатизации должен осуществляться контроль эффективности защиты персональных данных, а также оценка эффективности мер защиты персональных данных с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

	ФГБОУ ВО «Уральский государственный горный университет»	
	СТО « <i>Политика в отношении обработки персональных данных в ФГБОУ ВО «Уральский государственный горный университет»</i> »	
	СМК СТО 04-03.535-2025	Стр. 13 из 15

Ответственность за нарушения в области обработки и защиты персональных данных

Обязанности работников УГГУ, осуществляющих обработку и защиту персональных данных, а также их ответственность, определяются должностными инструкциями и положениями о структурных подразделениях УГГУ (для руководителей структурных подразделений), а также иными локальными нормативными актами УГГУ.

Утверждение, введение в действие и изменение Политики

10.1 Настоящая Политика утверждается ректором УГГУ.

10.2 УГГУ имеет право вносить изменения в настоящую Политику:

- по мере принятия новых нормативных правовых актов в сфере персональных данных или внесения в них изменений;

- по мере принятия локальных нормативных актов УГГУ, регламентирующие организацию обработки и обеспечение безопасности персональных данных.

10.3 Политика вступает в силу с момента ее утверждения приказом ректора.

Рассылка

Электронный образ настоящей Политики размещается на официальном сайте университета в информационно-коммуникационной сети «Интернет».

Подлинный печатный экземпляр Положения хранится в управлении лицензирования и аккредитации.

	Должность	Подпись	И. О. Фамилия
Политика разработана	Заместитель начальника центра компьютерных технологий		Д. В. Михеев
Положение зарегистрировано и соответствует СМК УОУ. УД. 04-06.60-2019 Управление документацией:	Начальник отдела контроля качества образования		

	ФГБОУ ВО «Уральский государственный горный университет»	
	СТО «Политика в отношении обработки персональных данных в ФГБОУ ВО «Уральский государственный горный университет»	
	СМК СТО 04-03.535-2025	Стр. 14 из 15

Лист согласования

Должность/подразделение	Подпись	И. О. Фамилия	Дата
Проректор по учебной работе		В. В. Зубов	
Начальник правового управления		А. И. Британов	
Начальник отдела кадров		Т. Б. Сабанова	

Приложение 1

Регистрация изменений, дополнений и ревизий документов

№ изменения	Дата внесения изменения, дополнения и проведения ревизий	Номера пунктов			Краткое содержание изменения, отметка о ревизии	Ф.И.О., подпись
		измененных	новых	аннулированных		
1	2	3	4	5	6	7