УТВЕРЖДАЮ:
Ректор ФГБОУ ВО "УГГУ"
_____ Н.П.Косарев
"31" 12. 2015 г.

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

СТАНДАРТ ОРГАНИЗАЦИИ

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

СМК СТО 5.05

Версия 2.0

Дата введения: «31» декабря 2015 г.

Екатеринбург – 2015

Содержание

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 – УГГУ) определяет основные подходы и требования к обработке и защите персональных данных (далее – ПДн) в УГГУ. Политика представляет собой систематизированное изложение целей, задач, принципов и условий обработки ПДн и действует в отношении любой информации о субъекте ПДн (физическом лице), которую УГГУ вправе обрабатывать.

2. Нормативные документы

Настоящая Политика разработана в соответствии с:

- Конституцией Российской Федерации,
- Трудовым кодексом Российской Федерации (ред. 05.10.2015),
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и иными нормативно-правовыми актами, регулирующими отношения, связанные с обработкой и защитой ПДн (ред.216-ФЗ и 242-ФЗ от 21.07.2014),
- Уставом УГГУ,
- Положением о защите персональных данных работников и обучающихся федерального государственного бюджетного образовательного учреждения высшего образования «Уральский государственный горный университет», утвержденного ректором УГГУ 6 декабря 2011 г.

3. Назначение Политики

Политика является методологической основой для:

- принятия управленческих решений и разработки практических мер по воплощению политики в отношении обработки ПДн и их защиты и выработки комплекса согласованных правовых, организационных, технических и иных мер, направленных на выявление угроз в отношении ПДн 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 ПДн;
- разработки предложений по совершенствованию правовых, организационных, технических и иных мер по обработке и защите ПДн в УГГУ;

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

Действие настоящей Политики распространяется на ПДн всех категорий субъектов ПДн, 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 ГЭК и ГАК;
- 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 ПДн в УГГУ

4.1. Основные цели Политики:

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

- установление ответственности должностных лиц УГГУ за невыполнение требований норм, регулирующих обработку и защиту ПДн.

4.2. Основные задачи Политики:

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

4.3. Принципы обработки ПДн в УГГУ:

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

5.1. Обработка ПДн в УГГУ осуществляется с соблюдением принципов, определенных п. 2.3 настоящей Политики.

5.2. Обработка ПДн допускается в следующих случаях:

- обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн, за исключением случаев, определенных федеральными законами;
- обработка ПДн необходима для осуществления и выполнения функций, полномочий и обязанностей, возложенных на УГГУ законодательством Российской Федерации, Уставом УГГУ и (или) договором;
- обработка ПДн 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 ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем;
- обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;
- обработка ПДн 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 ПДн;
- обработка ПДн 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 ПДн;
- осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн, либо по его просьбе;
- осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами.

5.3. Обработка специальных категорий ПДн, а также биометрических ПДн 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 ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключенного с этим лицом договора.

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

6. Основные принципы построения системы безопасности ПДн

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

6.2. Системность. Предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места ИСПДн 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 ПДн, то есть постановку задач по комплексной защите ПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и их систем защиты, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой ИСПДн. 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 ПДн на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн 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 ПДн 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 ИСПДн УГГУ. Излишние меры безопасности не должны приводить к экономической неэффективности, снижению эффективности работы персонала.

6.8. Персональная ответственность. Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его должностных обязанностей. В соответствии с этим принципом распределение прав и обязанностей сотрудников 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 ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

6.10. Исключение конфликта интересов. Предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников 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 ИСПДн;
- 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 трудозатрат 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 ПДн 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 соответствовать установленным нормам и требованиям по безопасности ПДн.

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

6.16. Обязательность контроля. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности ПДн на основе используемых систем и средств защиты ПДн, 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.

7. Меры и методы обеспечения требуемого уровня защиты информационных ресурсов

7.1. При обработке ПДн 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 ПДн, обрабатываемых в УГГУ, должно достигаться:

- назначением ответственных лиц за организацию обработки и обеспечение безопасности ПДн в каждом подразделении УГГУ;

- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов УГГУ по вопросам обеспечения безопасности информации;

- подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн и процессов их обработки;

- персональной ответственностью за свои действия каждого сотрудника, в рамках своих должностных обязанностей, имеющего доступ к информационным ресурсам УГГУ;

- осуществлением внутреннего контроля и/или аудита соответствия обработки ПДн в УГГУ Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, локальным актам УГГУ не реже 1 раза в три года;

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

- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн в УГГУ;

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

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

7.3. При обработке ПДн в ИСПДн необходимый уровень защиты должен достигаться:

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

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

- четким знанием и строгим соблюдением всеми пользователями ИСПДн УГГУ требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

- определением угроз безопасности ПДн при их обработке в ИСПДн 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.

8. Средства обеспечения безопасности ПДн

8.1. На технические средства защиты возлагается решение следующих основных задач:

- идентификация и аутентификация пользователей при помощи имен или 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 ИСПДн 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 ПДн (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 ПДн за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение ПДн, разрушение средств информатизации должен осуществляется контроль эффективности защиты ПДн, а также оценка эффективности мер защиты ПДн с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

9. Ответственность за нарушения в области обработки и защиты ПДн

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

10. Утверждение, введение в действие и изменение Политики

10.1. Настоящая Политика принимается Ученым советом УГГУ и утверждается приказом ректора УГГУ.

10.2. УГГУ имеет право вносить изменения в настоящую Политику:

- по мере принятия новых нормативных правовых актов в сфере ПДн или внесения в них изменений;
- по мере принятия локальных нормативных актов УГГУ, регламентирующие организацию обработки и обеспечение безопасности ПДн.

10.3. Политика вступает в силу с момента ее утверждения приказом ректора и подлежит размещению на сайте УГГУ для обеспечения доступа к ней всех заинтересованных лиц.

11. Рассылка

Рассылка осуществляется согласно листу рассылки и с указанием номеров учтенных экземпляров (УЭ).

Стандарт организации СМК СТО 5.05 «Политика в отношении обработки персональных данных в ФГБОУ ВО «УГГУ» разработан:

Начальник ЦКТ _____ А.С. Лылов
(подпись)

«29» декабря 2015 г.

Лист согласования

Должность	Подпись	И.О.Ф.	Дата
Проректор по УМК		М.Б.Носырев	30.12.2015 г.
Проректор по правовым вопросам		Л.А.Антропов	30.12.2015 г.
Начальник УМКО		Л.А.Гаврилова	30.12.2015 г.

ПРИЛОЖЕНИЯ

Приложение 1
СМК СТО 5.05-Пр01

Регистрация изменений, дополнений и ревизий документов

№ изменения	Дата внесения изменения, дополнения и проведения ревизии	Номера листов			Краткое содержание изменения, отметка о ревизии	Ф.И.О., подпись
		Заменённых	Новых	Аннулированных		
1	2	3	4	5	6	7