

Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ**



П О Л О Ж Е Н И Е О Р Г А Н И З А Ц И И

СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

Положение о работе

с соглашениями о конфиденциальности в ИРНИТУ

ОРИГИНАЛ

Содержание

1	Область применения.....	3
2	Нормативные ссылки.....	3
3	Термины, определения и сокращения	4
4	Ответственность.....	6
5	Общие положения	6
6	Порядок работы с конфиденциальной информацией контрагентов.....	7
	Приложение 1 Лист согласования Положения о работе с оглашениями о конфиденциальности в ИРННТУ	11
	Приложение 2 Лист регистрации изменений в Положение о работе с оглашениями о конфиденциальности в ИРННТУ	12
	Приложение 3 Лист ознакомления с Положением о работе с оглашениями о конфиденциальности в ИРННТУ	13

УТВЕРЖДЕНОприказом ректора

от «21» декабря 2022г. № 871-О

П О Л О Ж Е Н И Е О Р Г А Н И З А Ц И И**СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА**Положение о работе с соглашениями о
конфиденциальности в ИРНИТУ

Введено впервые

1 Область применения

1.1 Настоящее Положение о работе с соглашениями о конфиденциальности в ИРНИТУ (именуемое в дальнейшем - «Положение») направлено на регулирование порядка выполнения условий и хранения заключаемых в ИРНИТУ соглашений о конфиденциальности (договоров, содержащих положения о конфиденциальности) в рамках исполнения сотрудниками ИРНИТУ своих должностных и иных, связанных с работой в ИРНИТУ обязанностей.

1.2 Данное Положение устанавливает порядок обращения с конфиденциальной информацией, полученной ИРНИТУ от его контрагентов (партнеров) и определяет основные меры ее защиты с целью предотвращения нанесения ущерба экономической безопасности университета и его контрагентов вследствие неправомерного использования конфиденциальной информации (ее утраты, хищения, разглашения или фальсификации).

1.3 Требования данного Положения обязательны для выполнения всеми сотрудниками университета (включая сотрудников, заключивших договор ГПХ).

1.4 Данное Положение не распространяется на устанавливаемый государственными органами режим защиты сведений, составляющих государственную тайну Российской Федерации. Действие документа не распространяется на информацию, составляющую государственную тайну Российской Федерации.

2 Нормативные ссылки

Настоящее Положение разработано на основе следующих нормативных документов:

Конституция Российской Федерации;

Гражданский кодекс Российской Федерации;

Федеральный закон от 29.07.2004г. N 98-ФЗ «О коммерческой тайне»;

Федеральный закон от 27.07.2006г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27.07.2006г. N 152-ФЗ «О персональных данных»;

Указ Президента Российской Федерации от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера»;

Устав федерального государственного бюджетного образовательного учреждения высшего образования «Иркутский национальный исследовательский технический

университет»;

СТО 002 Порядок управления документированной информацией (документами) СМК.

3 Термины, определения и сокращения

3.1 В настоящем Положении применены следующие термины с соответствующими определениями:

Гриф ограничения доступа к документу (ограничительный гриф) - реквизит, свидетельствующий об особом характере информации документа и ограничивающий доступ к нему;

Документированная информация (документ) - 1. Структурированная информация, зафиксированная на носителе. 2. Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

Доступ к информации, составляющей коммерческую тайну - ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

Защита информации - правовые, организационные и технические меры, направленные на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации;

Информационная безопасность - состояние защищенности информационной среды университета, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства;

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

Информация - сведения (сообщения, данные), независимо от формы их представления;

Информация (сведения), составляющая коммерческую тайну - сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны;

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

Контрагент - сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

Контрагент университета - юридические и физические лица, с которыми взаимодействует университет при выполнении работ (оказании услуг) на основании заключенных договоров (соглашений, контрактов);

Конфиденциальная информация - документированная информация, доступ к которой ограничивается в соответствии законодательством Российской Федерации. Информация, требующая защиты;

Машинный носитель информации - материальный носитель или устройство, предназначенное для записи, хранения и считывания информации средствами вычислительной и (или) оргтехники - персональными компьютерами (рабочими станциями), серверами и другими техническими средствами;

Носители информации (сведений), составляющей коммерческую тайну - носители информации (сведений), составляющей коммерческую тайну;

Обладатель информации, составляющей коммерческую тайну - лицо, которое владеет информацией, составляющей коммерческую тайну, на законном основании, ограничило доступ к этой информации и установило в отношении ее режим коммерческой тайны;

Обработка сведений (информации) - получение, хранение, преобразование, комбинирование, передача или любое другое использование сведений (информации);

Передача информации, составляющей коммерческую тайну - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности;

Предоставление информации, составляющей коммерческую тайну - передача информации, составляющей коммерческую тайну и зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций;

Разглашение информации - несанкционированное доведение защищаемой информации до третьих лиц, не имеющих права доступа к этой информации;

Разглашение информации, составляющей коммерческую тайну - действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору;

Режим коммерческой тайны - правовые, организационные, технические и иные принимаемые обладателем информации, составляющей коммерческую тайну, меры по охране ее конфиденциальности;

Секрет производства (ноу-хау) - сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны. Секретом производства не могут быть признаны сведения, обязательность раскрытия которых либо недопустимость ограничения доступа к которым установлена законом или иным правовым актом;

Средства защиты информации - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих коммерческую тайну, и иных конфиденциальных сведений, средства, в которых они реализованы, а также средства контроля эффективности защиты информации;

Утрата конфиденциальных документов - выход (в том числе и временный) документов из владения ответственного за их сохранность работника, которому они были

доверены, вследствие чего эти документы, а равно содержащиеся в них сведения, стали, либо могли стать достоянием посторонних лиц;

Электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

Энергонезависимый машинный носитель информации - машинный носитель информации, информация в которых, в отличие от энергозависимых машинных носителей информации, сохраняется после отключения электропитания или их изъятия из устройств, в которые они устанавливаются.

3.2 В настоящем Положении используются следующие сокращения:

ГПХ – договор гражданско-правового характера;

ИРНИТУ - федеральное государственное бюджетное образовательное учреждение высшего образования «Иркутский национальный исследовательский технический университет», далее также – университет;

НИОКР – научно-исследовательские и опытно-конструкторские работы;

НИР – научно-исследовательские работы;

СМК - система менеджмента качества;

СТО - стандарт организации.

4 Ответственность

4.1 Ответственность за разработку, пересмотр, идентификацию внесенных изменений в данное Положение возложена на руководителя НИЧ.

4.2 Разработчик настоящего Положения осуществляет периодическую проверку (пересмотр) данного положения в установленном порядке согласно СТО 002 Система менеджмента качества. Порядок управления документированной информацией (документами) СМК.

4.3 Ответственность за выполнение требований данного Положения возложена на всех сотрудников университета согласно условиям настоящего Положения.

5 Общие положения

5.1 Цель данного Положения - определение основных мер защиты обращения с конфиденциальной информацией контрагентов с целью предотвращения возможного нанесения ущерба экономической безопасности университета и его контрагентов (партнеров).

5.2 Руководители структурных подразделений университета несут персональную ответственность за обеспечение режима соблюдения требований конфиденциальности на участке деятельности подразделения, организуют выполнение установленных Положением режимных требований, принимают меры по максимальному ограничению возможности ознакомления с информацией работников, которым по роду выполняемых ими должностных обязанностей она не требуется. Руководители, отвечающие за исполнение хоз.договоров, договоров НИР, НИОКР, а также иных договоров от имени ИРНИТУ несут персональную ответственность за соблюдения режима обращения с конфиденциальной информацией, установленных в данных договорах или в отдельных соглашениях о конфиденциальности. В вопросах сохранения коммерческой тайны и иных конфиденциальных сведений, предоставляемых университету контрагентами, следует руководствоваться действующим законодательством Российской Федерации, данным Положением, а также условиями

обеспечения охраны конфиденциальности, изложенными в соответствующих договорах и (или) соглашениях, заключенных с контрагентами.

6 Порядок работы с конфиденциальной информацией контрагентов

6.1 В процессе взаимодействия университета с юридическими и физическими лицами (по вопросам выполнения работ, услуг выполнения НИР, НИОКР), взаимодействия по вопросам научной, образовательной, международной и иной деятельности могут возникать и как правило возникают правоотношения, связанные с обеспечением конфиденциальности полученной от контрагентов информации. Как правило, юридические лица – Заказчики университета, соответствующие положению о конфиденциальности, включают в основной договор, либо в отдельное соглашение о сотрудничестве положения о конфиденциальности. Должностное лицо университета, либо сотрудник ГПХ, являющийся руководителем выполнения соответствующих работ/руководителем взаимодействия с контрагентом по какому-либо направлению деятельности, обязан ознакомиться с нормативными положениями соглашения о конфиденциальности/договора и обеспечить их соблюдение как им лично, так и подчиненными сотрудниками. Приоритет установленного порядка действий имеет соответствующее соглашение о конфиденциальности, либо договор, содержащий такие требования. В случае, если специальный порядок не установлен, необходимо руководствоваться настоящим Положением. Соглашения о конфиденциальности/договоры, содержащие соответствующие положения подлежат хранению в НИЧ.

6.2 Независимо от условий соглашений о конфиденциальности/договоров, содержащих соответствующие положения, ключевой обязанностью ответственного за соблюдение режима конфиденциальности является ограничение доступа к информации, фиксация лиц, допущенных к информации в силу привлечения к выполнению работ или в связи с иной необходимостью, обеспечение взаимодействия с представителями контрагента по всем вопросам, связанным с полученной информацией, в отношении которой контрагент установил требование о соблюдении ее конфиденциальности, включая возможное использование информации в публикации научных статей, размещения информации на сайте университета, в новостях и иных разделах и т.п. Ответственным исполнителям следует сохранять переписку с представителями контрагента (включая переписку по адресам электронной почты) в подтверждение согласования тех или иных действий, связанных с полученной от них информацией, в отношении которой установлен режим соблюдения ее конфиденциальности.

6.3 Руководитель структурного подразделения/ответственный исполнитель по договору:

- доводит до сведений подчиненных работников/сотрудников требования настоящего Положения и условия соглашений о конфиденциальности/других документов, регламентирующих порядок работы с конфиденциальной информацией, полученных от контрагентов университета в случае привлечения их к участию в выполнении договоров:

- предупреждает об ответственности за нарушение требований по работе с конфиденциальной информацией.

Руководителю структурного подразделения/ ответственному исполнителю следует издавать соответствующие распоряжения и письменно знакомить с ними привлекаемых работников/сотрудников, которые могут получить доступ к соответствующим сведениям.

6.4 Работники/сотрудники университета, допущенные к конфиденциальной информации, обязаны:

ИРНТУ	Положение о работе с оглашениями о конфиденциальности в ИРНТУ	Положение – 2022
<p>- знать и выполнять требования данного Положения и других документов, регламентирующих вопросы обеспечения режима обращения с конфиденциальной информацией;</p> <p>- не разглашать конфиденциальную информацию, полученную в результате выполнения своих должностных обязанностей;</p> <p>- соблюдать установленные в университете правила работы с документами, порядок их учета, хранения и уничтожения;</p> <p>- знакомиться только с теми документами и информацией, к которым получили доступ в силу своих должностных обязанностей;</p> <p>- во время работы с документами принимать меры к исключению возможности ознакомления с ними других лиц, не имеющих к ним прямого отношения;</p> <p>- пресекать действия других лиц, которые могут привести к разглашению конфиденциальной информации;</p> <p>- в нерабочее время, а также при кратковременном отсутствии на рабочем месте документы, содержащие конфиденциальную информацию, хранить в закрытом на замок шкафу (сейфе);</p> <p>- немедленно информировать руководителя структурного подразделения и начальника Управления по информационным технологиям о фактах утраты (недостачи) документов (отдельных листов), содержащих конфиденциальную информацию, ключей от сейфов (шкафов), фактах обнаружения неучтенных конфиденциальных документов, а также о фактах необоснованного интереса к сведениям, составляющим конфиденциальную информацию, со стороны лиц, не имеющих прямого отношения к работе с ними;</p> <p>- при увольнении, переводе по работе, убытии в отпуск, в длительную командировку (более 1 месяца) сдать документы, содержащие конфиденциальную информацию. непосредственному руководителю</p> <p>6.5 При обработке конфиденциальной информации с использованием средств вычислительной и оргтехники работники обязаны:</p> <p>- соблюдать правила разграничения доступа к охраняемым данным, неукоснительно выполнять требования нормативных документов по организации доступа к информационным ресурсам, организации парольной и антивирусной защиты;</p> <p>- не разглашать свои индивидуальные пароли на доступ к компьютерным, сетевым и иным информационным ресурсам, выполнять требования соответствующих администраторов вычислительной сети и администраторов автоматизированных (информационных) систем по смене паролей, не применять "простых" паролей, не оставлять в легкодоступных местах листы и конверты с паролями;</p> <p>- принимать меры к исключению ознакомления посторонних лиц с информацией, выводимой на экран дисплея;</p> <p>- при подготовке электронных документов, содержащих конфиденциальную информацию, в верхнем правом углу (колонтитуле) первого экранного листа проставлять пометку с соответствующим ограничительным грифом ("Коммерческая тайна" или "Конфиденциально");</p> <p>- не использовать (не загружать, не запускать и т.п.) для обработки конфиденциальной информации посторонние программные средства, не допущенные для применения в университете. При требовании операционной системы обновления установленного программного обеспечения обязательно его произвести;</p> <p>- при необходимости покинуть свое рабочее место провести стандартные процедуры выхода из системы и отключения компьютера (в рабочее время допускается инициализация экранной заставки, защищенной индивидуальным паролем, или блокировка доступа к компьютеру с использованием аппаратно-программных средств и электронных ключей, принятых для эксплуатации в университете);</p>		

ИРНИТУ	Положение о работе с оглашениями о конфиденциальности в ИРНИТУ	Положение – 2022
<p>- не допускать случаев передачи информации, составляющей коммерческую тайну, по незащищенным каналам передачи данных, через сеть Интернет и иные публичные сети (включая факс), а конфиденциальной информации по электронной почте в открытом виде;</p> <p>- не допускать применения средств криптографической защиты и защиты от несанкционированного доступа, не принятых в эксплуатацию в университете или не предусмотренных эксплуатационной (технической) документацией на информационные и автоматизированные системы;</p> <p>- в нерабочее время, а также при кратковременном отсутствии на рабочем месте хранить съемные машинные носители, содержащие коммерческую тайну и иные конфиденциальные сведения, в закрытом на замок сейфе (шкафу);</p> <p>- немедленно информировать руководителя структурного подразделения о фактах или возможности несанкционированного доступа к информации в локальной вычислительной сети (ЛВС) университета.</p> <p>6.6 Работникам, допущенным к конфиденциальной информации, запрещается:</p> <p>- снимать и изготавливать копии конфиденциальных документов (в том числе с электронных документов), делать из них выписки без разрешения руководителя структурного подразделения;</p> <p>- выносить за пределы здания документы и машинные носители с информацией, составляющей коммерческую тайну, и иными конфиденциальными сведениями без разрешения своего руководителя подразделения. В случае служебной необходимости выноса (вывоза) документов и носителей, содержащих коммерческую тайну, на срок командировки оформляется разрешение, которое подписывается советником ректора по безопасности. При этом в служебной записке указывается перечень документов (электронных документов на машинных носителях), отнесенных к коммерческой тайне/конфиденциальной информации;</p> <p>- обсуждать вопросы, содержащие конфиденциальную информацию в присутствии посторонних лиц;</p> <p>- сообщать устно или письменно кому бы то ни было конфиденциальную информацию, если это не обусловлено выполнением служебных обязанностей.</p> <p>6.7 Кроме того, работникам /сотрудникам запрещается:</p> <p>- подключать к компьютерам различного рода внешние устройства, устанавливать на компьютеры и (или) использовать программные продукты (программы), копировать на (с) внешние машинные носители программное обеспечение без разрешения руководителя подразделения, за исключением программного обеспечения, устанавливаемого в соответствии с нормативными документами университета;</p> <p>- самостоятельно, без разрешения руководителя подразделения, подключать (или допускать подключение) к ЛВС университета компьютеры (в том числе мобильные) представителей контрагентов и других организаций или физических лиц, прибывающих в университет.</p> <p>6.8 Возможность открытого оглашения (публикации) конфиденциальных сведений, обладателем которых является университет, в отношении которых университет не является обладателем (собственником), может осуществляться при наличии письменного согласия обладателя (собственника) этой информации на ее открытое оглашение (публикацию), а также в иных случаях, предусмотренных действующим законодательством Российской Федерации.</p> <p>6.9 Разглашение сведений, составляющих конфиденциальную информацию, или утрата документов, содержащих таковую, относится к числу грубых нарушений трудовых обязанностей.</p> <p>6.10 За разглашение конфиденциальных сведений контрагентов, составляющих коммерческую тайну, виновные лица несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.</p>		

Федерации. За разглашение конфиденциальных сведений, не составляющих коммерческую тайну контрагентов, утрату документов, содержащих такие сведения, а также за иные нарушения установленного в университете порядка учета, хранения, обращения с конфиденциальными документами и информацией, не содержащих коммерческой тайны, виновные несут дисциплинарную ответственность, применяемую к подобного рода нарушениям в соответствии с действующими в университете локальными нормативными актами.

6.11 По фактам разглашения (утраты) конфиденциальных сведений проводится служебное расследование. Служебное расследование может также назначаться по фактам грубого нарушения установленных правил обращения с конфиденциальной информацией. Для проведения служебного расследования приказом ректора назначается комиссия в составе не менее трех человек. Руководитель структурного подразделения, проверяемого по фактам разглашения (утраты) конфиденциальных сведений принимает активное участие в обеспечении работы комиссии.

Комиссия, проводящая служебное расследование:

- выясняет обстоятельства, причины разглашения сведений или утраты документов, а также способствовавшие этому условия;
- устанавливает лиц, виновных в разглашении сведений или утрате документов;
- принимает меры к розыску утраченного документа или предотвращению негативных последствий разглашения сведений.

Члены комиссии, проводящие служебное расследование, имеют право:

- производить осмотр помещений университета (сейфов, столов, шкафов, и т.д.);
- проверять конфиденциальную документацию, журналы учета конфиденциальных документов;
- опрашивать работников университета, виновных в утрате (разглашении), а также других работников, которые могут оказать содействие в установлении обстоятельств происшедшего и получать от них письменные объяснения;
- привлекать работников других структурных подразделений, не заинтересованных в исходе дела, для проведения отдельных действий служебного расследования по согласованию с их руководителями.

Служебное расследование проводится в минимально короткий срок, но не более 10 рабочих дней со дня назначения комиссии. В случаях, когда в течение данного срока утраченные документы не обнаружены, поиск их может быть прекращен.

По результатам расследования составляется заключение, в котором отражаются следующие вопросы:


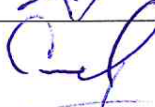




- основания для проведения расследования;
- кто и в какие сроки проводил расследование;
- перечень и результаты осуществленных мероприятий;
- виновные лица;
- выявленные причины и условия, способствовавшие разглашению (утрате);
- мнение о наличии в действиях виновного лица признаков административного правонарушения либо уголовно наказуемого деяния;
- возможные негативные последствия происшедшего для интересов университета и предложения по их устранению.

Заключение по результатам служебного расследования докладывается ректору университета для принятия решения о привлечении виновного к дисциплинарной ответственности либо о передаче материалов в правоохранительные или судебные органы, а также о мерах по устранению причин и возможных негативных последствий происшедшего либо об отклонении материалов расследования.


**Приложение 1 Лист согласования Положения о работе с оглашениями о
конфиденциальности в ИРНТУ**

(обязательное)

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Дата	Подпись
Проректор по цифровой трансформации	Копайгородский А.Н.	08.12.2022	
Проректор по учебной работе	Смирнов В.В.	08.12.2022	
Проректор по научной работе	Кононов А.М.	9.12.2022	
Руководитель юридической службы	Пенизева О.Л.	8.12.2022.	
Председатель профкома ИРНТУ	Пешков В.В.	9.12.2022	
Зам. начальника отдела мониторинга и качества образовательных услуг	Артемова О.С.	8.12.2022	

РАЗРАБОТАНО:

Начальник НИЧ	Калошин И.А.	07.12.2022.	
---------------	--------------	-------------	---

