СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

РАБОЧАЯ ИНСТРУКЦИЯ

РИ 6.5-6

Положение об организации и проведении
работ по обработке и защите
конфиденциальной информации

Регистрационный номер документа	
Структурное подразделение	
Уполномоченный по качеству	
Дата получения	

Комсомольск-на-Амуре
2014

РАБОЧАЯ ИНСТРУКЦИЯ

Система менеджмента качества **ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ И ПРОВЕДЕНИИ РАБОТ ПО ОБРАБОТКЕ И ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**	**РИ 6.5-6** **Введена впервые**

СОГЛАСОВАНО

Первый проректор

_____ И.В. Макурин

«28» 11 2014 г.

УТВЕРЖДАЮ

Ректор университета

_____ Э.А. Дмитриев

«28» ноября 2014 г.

Начальник ИТ-Управления

_____ Е.Б. Абарникова

«28» 11 2014 г.

Начальник организационно-правового управления

_____ Н.А. Лашкина

«28» ноября 2014 г.

Комсомольск-на-Амуре
2014

Введена приказом № 462а-О от 28.11.2014

Содержание

1 Назначение и область применения

1.1 Назначение

Настоящая инструкция определяет общий порядок обращений с документами на бумажных и иных материальных носителях информации, содержащими конфиденциальную информацию в ФГБОУ ВО «КнАГУ». **(Изм. № 1, 2)**

1.2 Сфера действия

Положение распространяется на порядок обращения со сведениями, составляющими конфиденциальную информацию (служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные). Положение не распространяется на порядок обращения со сведениями, составляющими государственную тайну.

1.3 Область применения

Настоящее положение должны использовать в своей работе все работники ФГБОУ ВО «КнАГУ», осуществляющие обработку конфиденциальной информации. **(Изм. № 1, 2)**

2 Нормативные ссылки

Настоящее положение разработано в соответствии со следующими нормативными документами:

Конституция Российской Федерации.

Трудовой кодекс Российской Федерации.

Кодекс об административных нарушениях Российской Федерации.

Гражданский кодекс Российской Федерации.

Уголовный кодекс Российской Федерации.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации».

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Постановления Правительства «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687.

Постановление Правительства «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 1 ноября 2012 г. № 1119.

Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18 февраля 2013 г. № 21.

Указ Президента Российской Федерации «Об утверждении перечня

сведений конфиденциального характера» от 06 марта 1997 г. № 188 (в ред. Указа Президента РФ от 23 сентября 2005 г. № 1111).

РИ 4.2.3-7 «О порядке обращения со служебной информацией ограниченного распространения в ФГБОУ ВО «КнАГУ». (**Изм. № 1, 2**)

3 Термины, определения, сокращения

3.1 Термины и определения

В настоящем положении применяются следующие термины с соответствующими определениями:

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством (за исключением информации, составляющей государственную тайну). К конфиденциальной информации относится служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные, сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Информация – сведения независимо от формы их представления.

Информационная безопасность – состояние и режим эксплуатации средств хранения, доставки и автоматизированной обработки, при котором обеспечивается уровень защиты информационных ресурсов, достаточный для минимизации ущерба, вызванного возможными нарушениями безопасности.

Информационный ресурс – различная информация Университета на всех этапах ее жизненного цикла, обеспечивающая основную деятельность Университета и представляющая ценность с точки зрения достижения поставленных целей.

Коммерческая тайна – режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. Под коммерческой тайной может также подразумеваться саму информацию, которая составляет коммерческую тайну, то есть, научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, в том числе составляющую секреты производства (ноу-хау), которая имеет действительную или потенциальную коммерческую ценность в силу

неизвестности её третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введён режим коммерческой тайны.

Конфиденциальный информационный ресурс – информационный ресурс, содержащий конфиденциальную информацию.

Объект доступа – любые конфиденциальные информационные ресурсы на носителях информации и в памяти средства вычислительной техники.

Персональные данные – любая информация, относящаяся прямо или косвенно определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Постороннее лицо – любое лицо, не имеющее непосредственного отношения к деятельности университета, посетители, работники других организационных структур.

Профессиональная тайна – информация, полученная гражданами (физическими лицами) при исполнении профессиональных обязанностей или организациями - при осуществлении определенных видов деятельности.

Работник – физическое лицо, состоящее в трудовых отношениях с работодателем.

Работодатель – ФГБОУ ВО «Комсомольский-на-Амуре государственный университет», выполняющий функции оператора персональных данных. (**Изм. № 1, 2**)

Руководство — Ректорат университета.

Служебная тайна (служебная информация ограниченного доступа) – конфиденциальная информация, образующаяся в процессе управленческой деятельности органа или организации, распространение которых препятствует реализации органом или организацией предоставленных ему полномочий, либо иным образом отрицательно сказывается на их реализации, а также конфиденциальные сведения, полученные органом или организацией в соответствии с их компетенцией в установленном законодательством порядке.

Субъект доступа к конфиденциальной информации – лицо, имеющее допуск к конфиденциальной информации.

Университет – ФГБОУ ВО «Комсомольский-на-Амуре государственный университет». (**Изм. № 1, 2**)

3.2 Сокращения

В настоящем положении применяются следующие сокращения:

КИ – конфиденциальная информация;

ИР – информационный ресурс;

РФ – Российская Федерация;

СВТ – средство вычислительной техники.

4 Ответственность

4.1 Работники университета, имеющие доступ к конфиденциальной информации, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования конфиденциальной информации.

4.2 Работники университета, виновные в нарушении норм, регулирующих получение, обработку и защиту конфиденциальной информации, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

4.3 Контроль над выполнением норм, регулирующих получение, обработку и защиту конфиденциальной информации, возлагается на руководство университета, начальника ИТ-управление, руководителей структурных подразделений университета, в которых осуществляется обработка конфиденциальной информации.

5 Общие положения

5.1 Конфиденциальная информация по условиям ее правового режима относится к информации ограниченного доступа и не относится к государственной тайне.

5.2 В соответствии с законодательством РФ к конфиденциальной информации относятся сведения, составляющие служебную тайну (служебная информация ограниченного доступа), профессиональную тайну, коммерческую тайну, банковскую тайну, персональные данные.

5.3 Информационные ресурсы, содержащие конфиденциальную информацию, сформированные в процессе деятельности ФГБОУ ВО «КнАГУ», а также приобретенные ФГБОУ ВО «КнАГУ» в собственность установленными законодательством РФ способами, являются собственностью ФГБОУ ВО «КнАГУ» и не могут быть использованы иначе как с разрешения собственника или в установленных законодательством РФ случаях. (**Изм. № 1, 2**)

5.4 Отнесение информации к конфиденциальной осуществляется в соответствии с перечнем сведений конфиденциального характера, составленным в соответствии с законодательством РФ.

5.5 Информация конфиденциального характера не может быть использована в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан.

5.6 В случае ликвидации ФГБОУ ВО «КнАГУ» решение о дальнейшем использовании конфиденциальной информации принимает ликвидационная комиссия. (**Изм. № 1, 2**)

6 Организация и проведение работ по обработке конфиденциальной информации

6.1 Работы по обработке информации, составляющей служебную тайну (служебная информация ограниченного доступа), осуществляются в соответствии с **РИ 4.2.3-7** «О порядке обращения со служебной информацией ограниченного распространения в ФГБОУ ВО «КнАГУ». (**Изм. № 1, 2**)

6.2 Работы по обработке информации, составляющей профессиональную тайну и коммерческую тайну, осуществляются в порядке, аналогичном порядку, изложенному в **РИ 4.2.3-7.**

6.3 Работы по обработке персональных данных осуществляются в соответствии с «Положением об обработке персональных данных».

6.4 Обязательными условиями обработки КИ с помощью СВТ являются:

– определение перечня служебных помещений, в которых установлены СВТ, предназначенные для обработки и хранения КИ;

– определение круга лиц, допущенных к ознакомлению и обработке КИ;

– учет носителей информации, на которых хранится КИ;

– персональный допуск сотрудников к работам на СВТ, путем использования персональных идентификаторов и паролей;

– возможность идентификации всех лиц, обращающихся к конфиденциальным ИР;

– резервное копирование конфиденциальных ИР;

– возможность применения дополнительных мер защиты информации.

6.5 Все конфиденциальные ИР подлежат обязательной регистрации в журнале учета конфиденциальных информационных ресурсов ФГБОУ ВО «КнАГУ», создаваемые путем сбора, ввода, приема информации, а также учету подлежит обрабатываемая конфиденциальная информация путем вывода (отображения, печати), передачи, записи, хранения, а также уничтожаемые конфиденциальные ИР. Допускается ведение автоматизированного учета и регистрации с использованием СВТ с обязательным резервным копированием данных. Носители КИ подлежат инвентарному учету в журналах учета. **(Изм. № 2)**

6.6 Ввод конфиденциальной информации с печатных документов и других источников должен осуществляться только на АРМ, предназначенных для обработки КИ, сотрудниками, имеющими допуск к работе с КИ. Создание конфиденциальных ИР путем объединения (агрегирования) информации из нескольких конфиденциальных ИР также является вводом и подлежит регистрации.

6.7 Прием КИ осуществляется путем получения ИР на носителях информации. При приеме КИ сверяются реквизиты носителя информации. В случае отсутствия на носителях файлов составляется акт в двух экземплярах, один из которых высылается отправителю. Ошибочно поступившие носители возвращаются отправителю.

Принимаемые электронные носители конфиденциальной информации в любом виде подлежат обязательной антивирусной проверке.

6.8 Вывод КИ осуществляется при печати ИР или отображении на устройствах вывода информации (мониторах, проекторах, экранах и т. д.). Вывод на печать конфиденциальных ИР должен быть явно разрешен руководством ФГБОУ ВО «КнАГУ» или лицом, назначенным руководством ФГБОУ ВО «КнАГУ» и имеющим соответствующие полномочия. Каждый печатный документ (в т. ч. черновик), подлежит регистрации. Вывод КИ разрешается только на СВТ, предназначенных для обработки КИ. **(Изм. № 1, 2)**

6.9 Передача КИ осуществляется при пересылке (передаче) электронного документа, содержащего КИ с СВТ на любое другое СВТ. Запись конфиденциального ИР осуществляется при копировании, перемещении ИР с места исходного хранения на любой другой носитель информации или после внесения изменений в исходный ИР и записи на носитель. Передача КИ должна санкционироваться руководством ФГБОУ ВО «КнАГУ» или лицом, назначенным руководством ФГБОУ ВО «КнАГУ» и имеющим соответствующие полномочия. Передача КИ разрешается только на СВТ, предназначенные для обработки КИ. **(Изм. № 1, 2)**

Каждый вид передаваемых конфиденциальных ИР (файл, электронный документ, сообщение и т.д.) должен иметь состав реквизитов определенных требованиями к оформлению документов. При подготовке передаваемого ИР количество копий определяет исполнитель и руководитель, санкционирующий передачу ИР, а количество копий, адресаты, фамилия исполнителя и его телефон указываются на носителе.

Передача носителей, содержащих КИ, от одного сотрудника другому осуществляется с разрешения руководства ФГБОУ ВО «КнАГУ» или лица, назначенного руководством ФГБОУ ВО «КнАГУ» и имеющим соответствующие полномочия, с отметкой в соответствующих журналах учета. **(Изм. № 1. 2)**

Запись конфиденциального ИР разрешается только на носители информации, предназначенные для хранения КИ, зарегистрированные и промаркированные в установленном порядке. Запрещается удалять (уничтожать) ИР на месте исходного хранения после копирования без прямого указания руководства ФГБОУ ВО «КнАГУ» или лица, назначенного руководством ФГБОУ ВО «КнАГУ» и имеющим соответствующие полномочия и

регистрации. Перемещение конфиденциального ИР (копирование без сохранения исходного ИР) должно сопровождаться необходимыми операциями по гарантированному уничтожению КИ на источнике. (**Изм. № 1, 2**)

Передача и запись конфиденциального ИР должна регистрироваться в журналах учета. Передача и запись КИ должна осуществляться только с СВТ, предназначенных для обработки КИ. При смене ответственного за эксплуатацию/ответственного за администрирование СВТ, составляется акт приема-сдачи носителей, содержащих КИ, который утверждается руководителем ФГБОУ ВО «КнАГУ». (**Изм. № 1, 2**)

6.10 Конфиденциальные ИР подлежат хранению только на выделенных для этой цели СВТ и носителях информации. Носители информации, используемые при создании резервных копий конфиденциальных ИР, подлежат хранению так же, как и основные копии. Хранение конфиденциальных ИР производится в течение срока, определяемого в соответствующей организационно-распорядительной документации. Носители информации, содержащие конфиденциальные ИР, подлежат хранению в специально выделенном для этой цели сейфе.

6.11 По истечении срока хранения производится уничтожение конфиденциальных ИР. Данные операции производятся ответственным за администрирование СВТ. При снятии категории конфиденциальных ИР, они удаляются (уничтожаются) с носителей и АРМ-ов, предназначенных для хранения и обработки КИ.

Съемные носители КИ, при отсутствии необходимости их хранения, подлежат уничтожению. При уничтожении КИ составляется перечень всех носителей и СВТ, содержащих данный ИР, производится уничтожение данных ИР и составляется акт.

7 Организация и проведение работ по защите конфиденциальной информации

7.1 Организация и проведение работ по защите конфиденциальной информации при ее обработке техническими средствами определяются данным Положением, иными нормативными документами ФГБОУ ВО «КнАГУ» по защите информации, действующим законодательством РФ, методическими документами Федеральной службы по техническому и экспортному контролю. (**Изм. № 1, 2**)

7.2 Защита конфиденциальной информации осуществляется путем выполнения комплекса мероприятий (правовых, организационных, технических) по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения,

по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Правительством РФ и федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, противодействия техническими разведкам и технической защиты информации, в пределах их полномочий.

7.3 Организация работ по защите конфиденциальной информации возлагается на ректора и начальника ИТ-Управления, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации – на специалистов по информационной безопасности ИТ-Управления.

7.4 Лица, осуществляющие обработку информации конфиденциального характера на СВТ обязаны соблюдать требования нормативных документов ФГБОУ ВО «КнАГУ» в части обработки конфиденциальной информации (служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные) и требований «Политики информационной безопасности», «Инструкции по обеспечению информационной безопасности на автоматизированных рабочих местах». (**Изм. № 1, 2**)

7.5 Для обработки конфиденциальной информации необходимо использовать СВТ с применением сертифицированных программных, технических и программно-технических средств защиты информации. Вычислительные комплексы обработки информации должны быть аттестованы/декларированы в соответствии с требованиями законодательства РФ по направлению защиты информации. Применяемое на СВТ программное обеспечение должно быть лицензионным.

7.6 Для передачи конфиденциальной информации по линиям связи за пределы контролируемой зоны ФГБОУ ВО «КнАГУ», необходимо использовать защищенные каналы связи с применением средств криптографической защиты информации. (**Изм. № 1, 2**)

7.7 Для разграничения доступа к конфиденциальной информации приказом ректора назначаются следующие субъекты доступа:

– пользователи СВТ для работы с КИ. Пользователями назначаются лица из числа сотрудников ФГБОУ ВО «КнАГУ» или сторонние лица, которым по решению руководства ФГБОУ ВО «КнАГУ» предоставлено разрешение на ознакомление или обработку конфиденциальной информации на СВТ; (**Изм. № 1, 2**)

– администраторы СВТ для работы с КИ. Администраторами назначаются лица из числа сотрудников ФГБОУ ВО «КнАГУ», которые осуществляют администрирование и поддержание работоспособности СВТ; (**Изм. № 1. 2**)

– администраторы безопасности СВТ для работы с КИ. Админи-

страторами безопасности назначаются лица из числа сотрудников ФГБОУ ВО «КнАГУ», которые осуществляют администрирование и поддержание работоспособности средств защиты информации, а также осуществляющие контроль выполнения требований по защите информации и исполнение организационной-распорядительных документов. (**Изм. № 1, 2**)

7.8 С целью соблюдения принципа персональной ответственности за свои действия каждому субъекту доступа сопоставляется персональный уникальный идентификатор (логин, имя пользователя), под которым он регистрируется и работает на СВТ. Субъекту доступа в случае производственной необходимости могут быть сопоставлены несколько идентификаторов. Использование несколькими субъектами доступа одного и того же идентификатора для работы с КИ (группового имени) запрещено.

7.9 Процедура регистрации (создания идентификатора и учетной записи) субъекта и предоставления ему (или изменения его) прав доступа к КИ инициируется заявкой субъекта. Заявка визируется руководством ФГОУ ВО «КнАГУ», чем подтверждается производственная необходимость доступа (изменения прав доступа) данного субъекта и допуска данного лица к КИ на СВИ. На основании заявки администратор производит необходимые операции по созданию (изменению, удалению) учетной записи, прав доступа и пароля. Субъекту под роспись сообщается идентификатор, пароль и передается персональный идентификатор (в случае использования в качестве идентификатора физического устройства). (**Изм. № 1, 2**)

7.10 Используемые пароли должны соответствовать правилам парольной защиты, изложенным в «Инструкции по обеспечению информационной безопасности на автоматизированных рабочих местах».

7.11 При наличии технологической необходимости в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п. использования идентификаторов и паролей некоторых сотрудников в их отсутствие, идентификаторы и пароли предоставляются администратором с указания руководителя ИТ-Управления. По окончанию работ, вызванных нештатной ситуацией и до момента возвращения сотрудника, учетная запись блокируется. При возвращении сотрудника к исполнению своих обязанностей, руководитель сотрудника направляет запрос в ИТ-Управление на разблокировку учетной записи сотрудника, после чего сотрудником задается новый пароль.

7.12 Хранение сотрудником своих паролей (в печатном виде) и персональных идентификаторов допускается только в опечатанном конверте в сейфе.

7.13 Администратору запрещается предоставлять доступ в нарушении правил разграничения доступа и требований по защите информации, изложенные в пп. 7.5-7.12, а также приостанавливать доступ к КИ, без по-

следующего незамедлительного уведомления субъекта доступа или руководителя подразделения субъекта доступа.

7.14 Субъектам доступа категорически запрещается:

– обрабатывать КИ на СВТ, не оснащенных средствами защиты информации, при отключенных или некорректно работающих средствах защиты информации;

– использовать КИ при ведении переговоров по незащищенным каналам связи;

– использовать КИ в личных целых;

– делать копии с конфиденциальных ИР и носителей, а также использовать различные технические средства для их записи без разрешения руководства ФГБОУ ВО «КнАГУ»; (**Изм. № 1, 2**)

– работать с КИ и носителями на дому;

– выносить носители информации, содержащие КИ, за пределы контролируемой зоны без разрешения руководства ФГБОУ ВО «КнАГУ»;

– сообщать устно или письменно кому бы то ни было (в том числе работникам ФГБОУ ВО «КнАГУ») КИ, если это не вызвано служебной необходимостью; (**Изм. № 1, 2**)

– делать записи, расчеты и заметки, содержащие КИ в личных тетрадях, блокнотах и на иных неучтенных носителях информации.

7.15 Проверка правил разграничения доступа, прав и полномочий доступа к конфиденциальной информации на СВТ, наличия носителей, содержащих конфиденциальную информацию, проводится один раз в год комиссией, назначаемой руководством ФГБОУ ВО «КнАГУ». Результаты проверки оформляются актом. (**Изм. № 1, 2**)

8 Права и обязанности субъектов доступа

8.1 Администратор и администратор безопасности имеет право приостанавливать доступ к КИ субъектам в случаях аварийных ситуаций, компрометации парольно-ключевой информации и по указанию руководства ФГБОУ ВО «КнАГУ» или начальника ИТ-Управления. **(Изм. № 1, 2)**

8.2 Администратор безопасности имеет право проверять наличие носителей КИ у пользователей, проводить контроль исполнения требований по защите информации и технологии обработки КИ.

8.3 Пользователь имеет право запрашивать доступ к КИ и информацию о требованиях и правилах обработки КИ.

8.4 Учет конфиденциальных ИР и носителей информации осуществляется лицом, назначенным приказом руководства ФГОУ ВО «КнАГУ». (**Изм. № 1, 2**)

8.5 Все субъекты обязаны:

– знать и выполнять требования настоящего Положения;

– знать состав Перечня сведений конфиденциального характера ФГБОУ ВО «КнАГУ»; (**Изм. № 1, 2**)

– хранить в тайне известную им КИ, информировать своего непосредственного руководителя о фактах нарушения порядка обращения с конфиденциальными ИР и носителями, и о попытках несанкционированного доступа к ним;

– знакомиться только с той КИ, к которой получен доступ в силу исполнения прямых служебных обязанностей;

– о допущенных нарушениях установленного порядка работы, учета и хранения КИ, а также о фактах разглашения КИ представлять письменные объяснения.

9 Разработчики

Данный документ разработали:

Начальник ИТ-Управления	Е.Б. Абарникова
Ведущий специалист по информационной безопасности ОССА ИТ-Управления	Д.С. Магола

Лист регистрации изменений

	Номер приказа, дата утверждения изменений	Количество страниц изменения	Дата получения изменения	Подпись уполномоченного по качеству
1	№ 100-О от 15.03.2016	-	15.03.2016	Короткова М.В.
2	№ 166-О от 10.04.2018	-	10.04.2018	Усова Т.И.