КЫРГЫЗ МАМЛЕКЕТТИК ТЕХНИКАЛЫК УНИВЕРСИТЕТ	Кыргызский государственный технический университет им. И.Раззакова
	СИСТЕМА ОБЕСПЕЧЕНИЯ КАЧЕСТВА ОБРАЗОВАНИЯ
	ДП 01 – 7

ОДОБРЕНО
На заседании Ученого Совета
КГТУ им. И. Раззакова
Протокол № 10
от «21» 06 2023 г.

УТВЕРЖДАЮ
Ректор КГТУ им. И. Раззакова
_____ Чыныбаев М.К.
Приказ № 1140
«21» 06 2023 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КЫРГЫЗСКОГО ГОСУДАРСТВЕННОГО ТЕХНИЧЕСКОГО УНИВЕРСИТЕТА ИМ. И.РАЗЗАКОВА

Бишкек 2023

ЛИСТ ИЗМЕНЕНИЙ

№ версии НПА	№ раздела/пункта или абзац, в котором внесены изменения и дополнения (с указанием страницы)	№ и дата протокола Ученого совета КГТУ
1		Протокол №10 от 21.06.2013 г.

1.Общие положения

1. Концептуальная схема информационной безопасности Кыргызского государственного технического университета им. И.Раззакова (далее – КГТУ) направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

2. Политика информационной безопасности КГТУ преследует цель по обеспечению следующих прав граждан:

- Каждый имеет право на неприкосновенность частной жизни, на защиту чести и достоинства;
- Каждый имеет право на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных, электронных и иных сообщений. Ограничение этих прав допускается только в соответствии с законом и исключительно на основании судебного акта;
- Не допускается сбор, хранение, использование и распространение конфиденциальной информации, информации о частной жизни человека без его согласия, кроме случаев, установленных законом;
- Каждому гарантируется защита, в том числе судебная, от неправомерного сбора, хранения, распространения конфиденциальной информации и информации о частной жизни человека, а также гарантируется право на возмещение материального и морального вреда, причиненного неправомерными действиями.

3. **Государственные секреты** - информация, хранящаяся и перемещаемая любыми видами носителей, затрагивающая обороноспособность, безопасность, экономические, научно-технические и политические интересы Кыргызской Республики, подконтрольная государству и ограничиваемая специальными перечнями и правилами, разработанными в соответствии нормативными правовыми актами Кыргызской Республики.

4. **Информация персонального характера (персональные данные)** - зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности. К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном положении, финансовом положении, состоянии здоровья и прочее.

5. **Кибербезопасность** - сохранение свойств целостности (которая может включать аутентичность и отказоустойчивость), доступности и конфиденциальности информации в объектах информационной инфраструктуры, обеспечиваемое за счет использования совокупности средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками и страхования, профессиональной подготовки, практического опыта и технологий.

6. Под **коммерческой тайной** понимаются не являющиеся государственной тайной сведения, связанные с производством, технологией, управлением, финансовой и другой деятельностью университета, разглашение которых может нанести ущерб его интересам.

7. **Системное программное обеспечение** - совокупность программного обеспечения для обеспечения работы вычислительного оборудования.

8. **Средство криптографической защиты информации** - программное обеспечение или аппаратно-программный комплекс, реализующий алгоритмы криптографических преобразований, генерацию, формирование, распределение или управление ключами шифрования.

9. **Третьи лица** - все лица, кроме субъекта персональных данных, ректора, оператора (специалиста) обработчика персональных данных.

10. Настоящая Политика информационной безопасности (далее - Политика) разработана с учетом следующих нормативно-правовых актов Кыргызской Неспублики и международных стандартов:

- Статья 29 Конституции Кыргызской Республики;
- Законы Кыргызской Республики «Об информации персонального характера», «Об электронной подписи», «Об электронном управлении», «О коммерческой тайне», «О защите государственных секретов Кыргызской Республики», «Об охране здоровья граждан в Кыргызской Республике» и «О наружном видеонаблюдении»;
- Требования к защите информации, содержащейся в базах данных государственных информационных систем, утвержденный Постановлением Правительства КР от 21 ноября 2017 года № 762 и др.

11. Работа по обеспечению информационной безопасности проводится в отделе обслуживания цифровой инфраструктуры (далее – ООЦИ) по следующим направлениям:

- разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности;
- выявление, оценка и прогнозирование угроз информационной безопасности;
- организация технической защиты информации, участие в проектировании систем защиты;
- проведение периодического контроля состояния информационной безопасности, учет и анализ результатов с выработкой решений по устранению уязвимостей и нарушений;
- контроль за использованием закрытых каналов связи и ключей с цифровыми подписями;
- организация плановых проверок режима защиты, и разработка соответствующей документации, анализ результатов, расследование нарушений;
- разработка и осуществление мероприятии по защите персональных данных;
- организация взаимодействия со всеми структурами, участвующими в их обработке, выполнение требований законодательства к информационным системам персональных данных, контроль действий операторов, отвечающих за их обработку.

12. Организационно-правовой статус сотрудников информационной безопасности:

- сотрудники имеют право беспрепятственного доступа во все помещения, где установлены технические средства с Информационными системами, право требовать от руководства подразделений и администраторов Информационной системы прекращения автоматизированной обработки информации, персональных данных, при наличии непосредственной угрозы защищаемой информации;
- имеют право получать от пользователей и администраторов необходимую информацию по вопросам применения информационных технологий, в части касающейся вопросов информационной безопасности;
- Службы внутреннего аудита, имеет право проводить аудит действующих и вновь внедряемых Информационных систем, программного обеспечения, на предмет реализации требований защиты и обработки информации, соответствию требований законодательства, запрещать их эксплуатацию, если не отвечают требованиям или продолжение эксплуатации может привести к серьезным последствиям в случае реализации значимых угроз безопасности;
- сотрудники имеют право контролировать исполнение утвержденных нормативных и организационно-распорядительных документов, касающихся вопросов информационной безопасности.

Область действия

13. Требования настоящей Политики распространяются на всех сотрудников КГТУ (штатных, временных, работающих по контракту и т.п). Положения настоящей Политики

применимы для использования во внутренних нормативных и методических документах, а также в договорах с контрагентами.

Порядок доступа пользователей к информационным системам, в которых обрабатывается информация персонального характера

14. Управление доступом к информационным системам реализовано с помощью штатных средств (операционных систем MS Windows Server, Linux и используемых ими СУБД) в целях идентификации и проверки подлинности субъектов доступа при входе в Информационную систему, а также для их регистрации входа (выхода) в систему (из системы).

15. Требование идентификации и аутентификации при входе в информационную систему определяется в законах Кыргызской Республики «Об информации персонального характера», «Об электронной подписи», «Об электронном управлении».

16. В составе информационных систем персональных данных используются сертифицированные или разрешенные к применению средства защиты информации от несанкционированного доступа.

17. Все действий пользователей информационной системы регистрируются в журналах событий системного и прикладного программного обеспечения. Данные электронные журналы доступны для чтения, анализа и резервного копирования только администратору соответствующего программного обеспечения, который несет персональную ответственность за полноту и точность отражения в журнале имевших место событий.

18. Любой доступ к базам данных информационных систем без фиксации в соответствующих журналах или лог-файлах запрещен. В случае увольнения сотрудника, имеющего права суперпользователя, пароли доступа к серверам и базам данных меняются в тот же день.

Сетевая безопасность

19. Доступ из Интернет в сеть университета:

- доступ во внутреннюю сеть осуществляется только через настроенный межсетевой экран;
- доступ из вне периметра сети разрешен только по распоряжению заведующего ООЦИ с согласованием с руководством университета, по определенному порту и на определенное время;
- не допускается удаленный доступ в локальную сеть с использованием не персонифицированных, групповых и анонимных учетных записей;
- не допускается использование программ удаленного администрирования типа TeamViewer.
- настройка и конфигурация средств обнаружения вторжений, межсетевых экранов должны обеспечивать оперативное обнаружение несанкционированного доступа к ресурсам сети для принятия мер блокирования проникновения нейтрализации последствий.

20. При администрировании удаленного доступа к ресурсам корпоративной сети КГТУ предъявляются следующие требования:

- удаленный доступ пользователей к ресурсам и сервисам компьютерной сети КГТУ обеспечивается на основе зарегистрированных персональных учетных записей, с использованием технологии VPN, других протоколов шифрования;
- делается соответствующая запись в журнале учета предоставления удаленного доступа;
- список сотрудников, которым предоставлен удаленный доступ поддерживается в актуальном состоянии и хранится в ООЦИ.

21. В целях обеспечения безопасности и нормального функционирования компьютерных сетей запрещается:

- самовольно подключать компьютерное оборудование (беспроводные точки доступа, маршрутизаторы, компьютеры и др.) к сети университета и присваивать ему сетевое имя и адрес без согласования с ООЦИ;

- перемещать компьютеры между сетевыми розетками и другими коммуникационными устройствами без согласования с ООЦИ;

- использовать информационные ресурсы университета для сетевых игр, распространения коммерческой рекламы; организации СПАМа.

- сканировать узлы сети неуполномоченными на то сотрудникам.

22. В КГТУ используется система межсетевого экранирования, которая реализует функции фиксации во внутренних журналах информации о проходящем IP-трафике, фильтрации пакетов служебных протоколов, блокирования доступа не идентифицированного объекта.

23. Подсистема обнаружения вторжений, обеспечивает выявление сетевых атак на элементы информационных систем, подключенные к сетям общего пользования и (или) международного обмена.

24. Функционал подсистемы реализуется программными и программно-аппаратными средствами на межсетевых экранах. Администратор сети ведет протоколирование и регулярный мониторинг доступа, контролирует содержание трафика с использованием специализированного программного обеспечения, проводит анализ лог-файлов.

25. На межсетевом экране заводится лог-файл, куда записываются все обращения к ресурсам (попытки создания соединений). Доступ к лог-файлам имеют администратор сети.

26. Анализ лог-ф файлов проводится с применением соответствующего программного обеспечения (анализатор логов) администратором сети. Администратор сети должен иметь независимый доступ к элементам системы защиты для контроля настроек конфигураций, просмотра системных журналов.

27. Доступ из одного сегмента сети в другой ограничивается и разделяется маршрутизаторами. Настройкой маршрутизаторов занимается ООЦИ.

28. Приобретение и установка средств и систем защиты информационных систем осуществляются по согласованию с заведующим ООЦИ. Сеть информационных систем персональных данных выделена в отдельный сегмент и защищена межсетевым экраном.

Локальная безопасность

29. Исходя из Требования к защите информации, содержащейся в базах данных государственных информационных систем, утвержденный Постановлением Правительства КР от 21 ноября 2017 года № 762, антивирусная защита предназначена для обеспечения антивирусной защиты серверов и автоматизированном рабочем месте пользователей КГТУ.

30. На каждом работающем компьютере, или сервере при вводе в эксплуатацию или после переустановки операционной системы сотрудниками ООЦИ в обязательном порядке устанавливается и активируется антивирусная программа. Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на автоматизированном рабочем месте, серверах, осуществляется специалистами ООЦИ в соответствии с руководствами по применению конкретных антивирусных средств. Отключение или не обновление антивирусных средств не допускается. Установка и обновление антивирусных средств в КГТУ контролируется сотрудниками ООЦИ.

31. Не допускается присутствие и использование программного обеспечения и данных, не связанных с выполнением конкретных функций в бизнес-процессах КГТУ. Устанавливаемое или изменяемое программное обеспечение должно быть предварительно проверено на отсутствие вирусов. После установки или изменения программного обеспечения должна быть выполнена антивирусная проверка.

32. При обнаружении компьютерного вируса необходимо приостановить работу, проинформировать руководство и организовать устранение последствий вирусной атаки.

33. Ответственность за выполнение требований инструкции по антивирусной защите должна быть возложена на специалистов ООЦИ, а обязанности по выполнению мер антивирусной защиты должны быть возложены на каждого сотрудника КГТУ, имеющего доступ к цифровой инфраструктуре.

Разграничение прав доступа к информационным системам и системам хранения данных, защита от несанкционированного доступа

34. Для доступа к информационным системам КГТУ сотрудник и студент должны ввести логин и пароль.

35. При предоставлении доступа к операционным системам, приложениям информационной системе реализуется принцип минимума привилегий доступа.

36. В целях защиты информации организационно и технически разделяются подразделения КГТУ, имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности и смысловой направленности). Данная задача решается с использованием возможностей конкретных информационных систем, где в целях обеспечения защиты данных доступ и права пользователей ограничивается набором прав и ролей. В случае обработки информации конфиденциального характера права назначаются администратором информационных систем по ролевой матрице доступа, в соответствии с функциональными обязанностями, определяемыми должностью и по служебной записке руководителя подразделения согласованной с ООЦИ.

37. Администратором информационных систем проводится анализ журналов доступа к ресурсам информационных систем, фиксируются попытки несанкционированного доступа, о которых докладывается руководителю ООЦИ.

38. Не допускается использование учетных записей уволенных сотрудников.

39. Пользователям (сотрудникам и студентам) запрещается передавать данные своей учетной записи (логин и пароль) третьим лицам. В случае передачи своего логина и(или) пароля третьему лицу, пользователь несет ответственность за несанкционированные действия третьего лица, как за свои собственные.

Использование электронной почты, сети Интернет

40. Не допускается распространять материалы, использование и распространение которых ограничено действующим законодательством Кыргызской Республики.

41. Пересылка информации конфиденциального характера осуществляется только с использованием корпоративной почты.

42. Электронная почта на рабочем месте сотрудника используется только для служебной, и иной, предусмотренной должностными обязанностями переписки.

43. Логин и пароль к корпоративной электронной почте для сотрудников выдает ответственный сотрудник департамента IT-Технологий по служебной записке на имя руководителя департамента IT-Технологий, для студентов по студенческому билету.

44. Запрещается открывать письма с подозрительными вложениями, с незнакомого адреса и т.п. о получении подобных писем сообщается комплаенсу.

45. Запрещается публиковать информацию конфиденциального характера в социальных сетях, пересылать через системы мгновенного обмена сообщениями (Skype, ICQ, Jabber и. т.п.).

46. Запрещается использование облачных сервисов на рабочих местах сотрудников, обрабатывающих информацию конфиденциального характера.

47. Доступ через беспроводную сеть разрешается только к общедоступным ресурсам сети. Беспроводные точки устанавливают и администрируют сотрудники ООЦИ.

48. Самостоятельно скачивать и устанавливать программное обеспечение разрешается только уполномоченным на то сотрудникам ООЦИ.

49. Запрещается несогласования с ООЦИ установка роутеров WiFi.

Обработка персональных данных

50. Необходимая нормативная и организационно-регламентирующая документация размещена на сайте КГТУ.

51. Все сотрудники КГТУ, являющиеся пользователями информационной системы персональных данных, должны четко знать и строго выполнять установленные законами КР "Об информации персонального характера", "Об электронной подписи", «Об электронном управлении» и «О наружном видеонаблюдении» правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности обработки персональных данных.

52. Компетентность пользователей в области обеспечения информационной безопасности достигается обучением правилам безопасной (с точки зрения информационной безопасности) работы, осведомленности об источниках потенциальных угроз и периодическими проверками их знаний и навыков. Занятия с пользователями проводятся комплаенс и/или уполномоченным государственным органом в области государственной и национальной безопасности (КГНБ КР) на регулярной основе не реже двух раз в год.

53. Все действия пользователей компьютеров и обязанности по соблюдению требований информационной безопасности определяются Соглашением (договором) о неразглашении конфиденциальной информации (Приложение 1), который они изучают, имеют распечатанный экземпляр с подписью сотрудника об ознакомлении.

54. При запуске сотрудника к выполнению обязанностей связанных с обработкой персональных данных непосредственный начальник подразделения, в которое он поступает, организует ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, подает служебную записку руководителю ООЦИ о предоставлении доступа к информационным системам персональных данных с указанием предполагаемой роли сотрудника.

55. Далее сотрудник проходит инструктаж у администратора безопасности информационных систем персональных данных, и расписывается об ознакомлении с Соглашением (договором) о неразглашении конфиденциальной информации (Приложение 1), получает у администратора информационной системы персональных данных, логин и пароль к учетной записи с правами ролевой матрицы доступа.

56. Порядок работы с запросами на предоставление сведений по персональным данным определяется Порядком получения согласия субъекта персональных данных па сбор и обработку его персональных данных, порядок и форму уведомления субъектов персональных данных о передаче их персональных данных третьей стороне, утвержденным Постановлением Правительства КР от 21 ноября 2017 года № 759.

57. С согласия субъекта персональных данных общедоступными персональными данными сотрудников являются фамилия, имя, отчество, занимаемая должность, подразделение, а студентов, аспирантов, докторантов, слушателей - фамилия, имя, отчество, группа, направление/специальность.

58. Сотрудники КГТУ должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

59. Сотрудникам, обрабатывающим персональные данные, запрещается устанавливать любое программное обеспечение, подключать личные мобильные устройства и отчуждаемые незарегистрированные в Службе внутреннего аудита носители информации, а также записывать на них защищаемую информацию, за исключением случаев, предусмотренных функциональному обязанностями.

60. Сотрудникам запрещается разглашать содержание защищаемой информации, которая стала им известна при работе с информационными системами КГТУ, третьим

лицам, согласно законами КР "Об информации персонального характера", "Об электронной подписи", «Об электронном управлении» и «О наружном видеонаблюдении».

61. Запрещается хранение информации конфиденциального характера локально на компьютере, не оснащенном программными средствами предотвращения несанкционированного доступа (SecretNet. DallasLock и др.).

62. Доступ к Информационным системам персональных данных третьих лиц для осуществления ими договорных обязательств осуществляется при выполнении требований, предъявляемых к защите информации и соблюдения конфиденциальности, отражаемых в договоре, согласованном Службой внутреннего аудита на этапе заключения.

63. Средства криптографической защиты информации при обработке персональных данных не используются.

Дублирование, резервное копирование и хранение информации

64. Все информационные данные КГТУ, включая сайт университета, образовательный портал AVN, 1С: Предприятие, и др. хранятся в системе хранения данных, которая находится в серверной университета. Кроме этого, эти данные также хранится в облачном диске.

65. Для обеспечения физической целостности данных, во избежание умышленного или неумышленного уничтожения, или искажения защищаемой информации и конфигураций информационных систем организуется резервное копирование баз данных, конфигураций, файлов настроек, конфигурационных файлов.

66. Порядок резервного копирования, дублирования, хранения архивов и восстановления информации определен Требованием к защите информации, содержащейся в базах данных государственных информационных систем, утвержденный Постановлением Правительства КР от 21 ноября 2017 года № 762.

67. Для обеспечения гарантированного восстановления особо важной информации, которая может быть утеряна вследствие аппаратных сбоев, воздействия вирусов-шифровальщиков проводится ежедневное резервное копирование содержимого дисков. В день 3 раза все информационные данные КГТУ копируются на систему хранения данных и один раз в день передается в хранение под облачное пространство – облачный диск. Ответственными за организацию резервного копирования, хранения копий и восстановления информации являются администраторы информационных систем, ответственные сотрудники ООЦИ.

68. Доступ к резервным копиям организуется по протоколу ftps и SMB для Acronis Storage Server. Еженедельно архивная копия базы данных информационных систем персональных данных дублируется сотрудником ООЦИ с использованием соответствующего оборудования на отчуждаемый носитель.

Ответственность за соблюдение положений Политики информационной безопасности

69. Общее руководство обеспечением информационной безопасности осуществляет руководитель Службы внутреннего аудита.

70. Ответственным за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение и внесение изменений в процессы информационной безопасности является руководитель ООЦИ.

71. Нарушение требований Политики, локальных нормативных актов по обеспечению информационной безопасности является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Кыргызской Республики, локальными нормативными актами, договорами, заключенными между КГТУ и сотрудниками (студентами, аспирантами).

72. Степень ответственности за нарушение требований локальных нормативных актов в области информационной безопасности определяется в каждом конкретном случае.

73. Руководители структурных подразделений, несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях и обязаны незамедлительно сообщать в Службу внутреннего аудита и руководителю ООЦИ, о всех инцидентах, связанных с нарушениями требований информационной безопасности.

74. Руководитель ООЦИ обязан незамедлительно сообщить в Службу внутреннего аудита, о всех происшествиях и нештатных ситуациях в области информационной безопасности.

75. Виды ответственности, предусмотренные законами Кыргызской Республики:

- гражданско-правовая ответственность;
- дисциплинарная ответственность;
- уголовная ответственность;
- административная ответственность.

Порядок пересмотра Политики информационной безопасности

76. Пересмотр Политики информационной безопасности производится не реже одного раза в три года и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

77. Внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

78. Изменения и дополнения в Политику утверждает ректор КГТУ.

СОГЛАСОВАНО:
Зав. ОПР  Исраилов А.Ж.

Приложение 1

Соглашение (договор) о неразглашении конфиденциальной информации

г. Бишкек « ____ » _____20___ г.

Учреждение «Кыргызский государственный технический университет им. И.Раззакова» (далее-университет), в лице Чыныбаева М.К., действующего на основании Устава и Политики информационной безопасности, и гражданином

_____
(фамилия, имя, отчество)

действующий от своего имени, именуемые в дальнейшем сторонами, заключили настоящее соглашение о нижеследующем:

Я, _____
(фамилия, имя, отчество)

будучи поставлен(а) в известность о том, что по роду своей служебной деятельности и должностным обязанностям буду допущен(а) к сведениям ограниченного распространения (персональные данные, коммерческая тайна, государственная тайна, секретные научные исследования, врачебная тайна, военная тайна и т.п.) в университете, принимаю на себя добровольные обязательства:

- не разглашать сведения ограниченного распространения, которые мне будут доверены (станут известны) по ходу службы;
- не передавать третьим лицам и не раскрывать публично сведения ограниченного распространения, без соответствующей санкции (разрешения) руководства;
- не передавать данные своей учетной записи (логин и пароль) третьим лицам;
- выполнять относящиеся ко мне требования приказов, инструкций и положений по защите сведений ограниченного распространения;
- в случае попытки посторонних лиц получить от меня сведения ограниченного распространения, немедленно сообщить об этом факте руководству своего подразделения;
- сохранять сведения ограниченного распространения сторонних организаций, с которыми университет связан договорными отношениями;
- не использовать знания сведений ограниченного распространения, для занятия какой-либо деятельностью, которая может нанести ущерб интересам университета;
- в случае моего увольнения, все носители сведений ограниченного распространения, которые находились в моем распоряжении в связи с исполнением своих служебных обязанностей, передать по указанию руководителя подразделения;
- об утрате или недостаче носителей сведений ограниченного распространения, что может привести к несанкционированными распространению конфиденциальных сведений, немедленно сообщить руководителю своего подразделения.

Обязуюсь добросовестно выполнять свои обязательства по настоящему соглашению.

Я предупрежден(а), что в случае невыполнения взятых на себя обязательств, могу быть привлечен(а) к ответственности в соответствии с действующим законодательством Кыргызской Республики и другими нормативными документами, действующими в университете.

Руководство обязуется, в случае допуска гр.:

_____
(фамилия, имя, отчество)

к сведениям ограниченного распространения, создавать необходимые условия для работы с такими сведениями.

_____ Ректор _____ **М. К. Чыныбаев**

Подпись лица,
заключившего соглашение