ПРИНЯТО
Решением Ученого Совета
ФГБОУ ВО КубГМУ Минздрава России
Протокол № 7 от «27» июня 2024 года

УТВЕРЖДАЮ
Ректор ФГБОУ ВО КубГМУ Минздрава России
_____ С.Н. Алексеенко
«27» июня 2024 года

Положение о защите конфиденциальной информации
ФГБОУ ВО КубГМУ Минздрава России

1. Общие положения

1.1. Положение о защите конфиденциальной информации ФГБОУ ВО КубГМУ Минздрава России (далее соответственно – Положение, Университет) регулирует отношения, связанные с обработкой конфиденциальной информации, создаваемой и (или) используемой в деятельности Университета, в отношении которой Университет является обладателем информации.

1.2. В целях защиты конфиденциальности в Положении нормативно устанавливаются способы определения конфиденциальной информации Университета, определения общих требований по обработке конфиденциальной информации, а также порядок разрешительной системы доступа к конфиденциальной информации, как основы ограничения доступа к конфиденциальной информации.

1.3. Университет руководствуется следующими основными принципами в вопросах ограничения доступа к конфиденциальной информации:

1.3.1. законность ограничения доступа – выполнение требований законодательства при отнесении информации (сведений, данных) к конфиденциальной информации. При этом учитываются как нормы, предписывающие налагать ограничения на доступ к этим сведениям, так и запрещающие такие ограничения;

1.3.2. обоснованность ограничения доступа – установление путем экспертной оценки работниками Университета отнесения информации к отдельным видам сведений, исходя из законных интересов Университета и в соответствии с принятыми в Университете локальными нормативными актами;

1.3.3. своевременность ограничения доступа – установление ограничений на разглашение и (или) распространение сведений с момента их получения (разработки) или заблаговременно.

1.4. В соответствии со статьей 6 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» действие Положения направлено на введение в Университете разрешительной системы доступа к конфиденциальной информации допускаемых лиц (далее – разрешительная система доступа).

1.5. Положение разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», иными нормативными правовыми актами Российской Федерации, Уставом и Положением ФГБОУ ВО КубГМУ Минздрава России по выявлению, обеспечению правовой охраны, учёту и использованию результатов интеллектуальной деятельности,

созданных при выполнении научно-исследовательских, научно-конструкторских и технологических работ.

2. Основные понятия, используемые в Положении

В Положении используются следующие понятия:

2.1. **информация** – сведения (сообщения, данные) независимо от формы их представления (текстовая, числовая, графическая, аудио, видео, электронная), в том числе:

2.1.1. данные – сведения, зафиксированные в какой-либо форме;

2.1.2. сообщения – сведения в какой-либо форме, передаваемые между участниками информационного взаимодействия;

2.2. **документированная информация** – информация, зафиксированная на материальном носителе (в том числе на бумажной основе) путем документирования с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

2.3. **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;

2.4. **конфиденциальность информации** – требование не разглашать информацию третьим лицам без согласия ее обладателя, обязательное для выполнения лицом, получившим доступ к определенной информации;

2.5. **конфиденциальная информация** – сведения в любой объективной форме, доступ к которым ограничивается в соответствии с Положением и разглашение которых может нанести материальный, репутационный или иной ущерб интересам Университета, его работников и обучающихся, и в отношении которой Университетом введен режим конфиденциальности информации.

2.6. **организация работы с документированной конфиденциальной информацией** – организация процессов учета, воспроизведения (копирования), предоставления, исполнения, отправления, классификации, систематизации, подготовки для оперативного и архивного хранения, уничтожения, хранения, проверки наличия и сохранности документированной конфиденциальной информации;

2.7. **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.8. **информация, составляющая коммерческую тайну** – техническая, производственная, финансово-экономическая, коммерческая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, и позволяет ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение или получить преимущество на рынке товаров, работ, услуг или получить иную коммерческую выгоду, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим ограничения доступа;

2.9. **иные сведения конфиденциального характера Университета** – сведения в любой объективной форме, создаваемые и используемые работниками Университета, а также физическими лицами – исполнителями по гражданско-правовым договорам, при исполнении трудовых(функциональных) обязанностей;

2.10. **обладатель информации** – юридическое лицо (Университет или его контрагент) или физическое лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

2.11. **допуск к конфиденциальной информации** – выполнение обладателем информации (уполномоченными должностными лицами) определенных процедур, связанных с оформлением права на доступ допускаемых лиц к конфиденциальной информации. Получение допуска со стороны допускаемого лица носит добровольный характер и является подтверждением с его стороны выполнения налагаемых обязательств. Наличие допуска предоставляет допускаемому лицу право работать с конфиденциальной информацией в объеме, определяемом обладателем информации;

2.12. **доступ к конфиденциальной информации** – практическая реализация предоставленного допуском права на возможность получения информации и ее использование (получение возможности ознакомления, в том числе с помощью технических средств, обработки, в частности, копирования, модификации или уничтожения);

2.13. **разрешительная система доступа** – совокупность правовых норм и требований, устанавливаемых обладателем информации с целью обеспечения правомерного ознакомления допускаемыми лицами с конфиденциальной информацией и ее использования для выполнения функциональных обязанностей. Разрешительная система доступа допускаемых лиц предусматривает установление в Университете единого порядка обращения с носителями сведений, составляющих конфиденциальную информацию, определение ограничений на доступ к ним различных категорий работников и иных допускаемых лиц, и степени ответственности за сохранность указанных носителей сведений.

2.14. **разглашение конфиденциальной информации** – действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя конфиденциальной информации;

2.15. **уничтожение конфиденциальной информации** – действия, направленные на приведение конфиденциальной информации в состояние, исключающее возможность ее использования и восстановления, в том числе посредством физического уничтожения и/ или удаления из памяти электронно-вычислительных машин носителей конфиденциальной информации и их копий;

2.16. **утрата конфиденциальной информации** – наносящее ущерб Университету состояние конфиденциальной информации, к которому приводят хищение и/ или потеря носителя конфиденциальной информации, несанкционированное уничтожение носителей конфиденциальной информации или только отображенной в них конфиденциальной информации, искажение или блокирование конфиденциальной информации;

2.17. **утечка конфиденциальной информации** – неправомерный (неразрешенный) выход такой информации за пределы защищаемой зоны ее функционирования в Университете или установленного круга лиц, имеющих право работать с ней, если этот выход привел к получению информации (ознакомлению с ней) лицами, не имеющими к ней санкционированного доступа. К утечке конфиденциальной информации приводит, в том числе, ее несанкционированное разглашение или распространение;

2.18. **информационные технологии** – процессы, методы поиска, сбора,

хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

2.19. **информационные ресурсы** – совокупность данных, организованных для получения информации. Под информационными ресурсами подразумеваются отдельные документы, массивы документов, базы данных в информационных системах, архивах, хранилищах, в том числе на носителях информации;

2.20. **несанкционированный доступ** – доступ к информации, нарушающий правила разграничения доступа с использованием или без использования штатных средств информационных систем;

2.21. **работник Университета** – физическое лицо, вступившее в трудовые отношения с университетом;

2.22. **обучающийся** – физическое лицо, осваивающее образовательную программу.

3. Порядок отнесения информации к категории конфиденциальной

3.1. Конфиденциальной информацией в Университете признаются следующие сведения:

3.1.1. Персональные данные, обрабатываемые Университетом;

3.1.2. Секреты производства (ноу-хау), сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них, сведения о научно-исследовательских работах, опытно-конструкторских и технологических работах, в результате которых есть вероятность создания объекта интеллектуальной собственности, а также иная информация, составляющая коммерческую тайну Университета;

3.1.3. Иные сведения конфиденциального характера, признанные Университетом как подлежащие защите, и разглашение которых может нанести материальный, репутационный или иной ущерб Университету, его работникам и обучающимся, в том числе указанные в Приложении к Положению.

3.2. Не относятся к конфиденциальной информации сведения:

3.2.1. содержащихся в учредительных документах Университета, документах, подтверждающих факт внесения записей об Университете в соответствующий государственный реестр;

3.2.2. о составе имущества Университета и об использовании средств соответствующих бюджетов;

3.2.3. о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

3.2.4. о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

3.2.5. о задолженности по выплате заработной платы и социальным выплатам;

3.2.6. о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

3.2.7. о размерах и структуре доходов и расходов Университета, о размерах и составе его имущества;

3.2.8. о перечне лиц, имеющих право действовать без доверенности от имени

Университета;

3.2.9. обязательность раскрытия, которых или недопустимость ограничения доступа, к которым установлена федеральными законами.

3.3. Отношения Университета и физических лиц, возникающие в связи с обработкой их персональных данных в Университете, регулируются Положением о порядке обработки персональных данных субъектов персональных данных ФГБОУ ВО КубГМУ Минздрава России.

3.4. Порядок оформления исключительных прав Университета на секреты производства (ноу-хау), изобретения, полезные модели, промышленные образцы и иные объекты интеллектуальной собственности, их правовая охрана, установление и обеспечение в Университете режима коммерческой тайны в отношении секретов производства (ноу-хау), изобретений, полезных моделей, промышленных образцов и иных объектов интеллектуальной собственности, а также особенности взаимоотношений Университета с работниками и третьими лицами в связи с использованием перечисленных результатов интеллектуальной деятельности устанавливается Положением ФГБОУ ВО КубГМУ Минздрава России по выявлению, обеспечению правовой охраны, учёту и использованию результатов интеллектуальной деятельности, созданных при выполнении научно-исследовательских, научно-конструкторских и технологических работ и иными локальными актами.

3.5. Сводный перечень сведений конфиденциального характера Университета представлен в Приложении к Положению. Руководители структурных подразделений, в деятельности которых присутствуют процессы обработки конфиденциальной информации, имеют право на подачу заявки на актуализацию указанного перечня.

3.6. Сведения, которые были получены Университетом от третьих лиц и в отношении которых третьими лицами заявлено, что они являются их конфиденциальной информацией, или конфиденциальный характер которых следует из законодательства Российской Федерации, подлежат защите наряду с конфиденциальной информацией Университета.

3.7. Режим конфиденциальности информации Университета действует:

3.7.1. для персональных данных, обрабатываемых Университетом, – до прекращения деятельности Университета;

3.7.2. для секретов производства (ноу-хау), сведений о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них, сведений о научно-исследовательских работах, иных сведений конфиденциального характера, – в течение срока, определенного нормами действующего законодательства и нормами локальных актов;

3.7.3. для информации, полученной от контрагентов Университета, – в течение срока, определенного соглашением о неразглашении конфиденциальной информации или иным договором.

4. Общие требования по обработке конфиденциальной информации

4.1. Обработка конфиденциальной информации включает в себя процессы подготовки и изготовления конфиденциальной информации, организации работы с конфиденциальной информацией и защиты конфиденциальной информации.

4.2. В Университете, в зависимости от форм представления конфиденциальной информации, регламентируются следующие направления обработки конфиденциальной информации:

4.2.1. обработка речевой и (или) звуковой конфиденциальной информации;

4.2.2. обработка недокументированной конфиденциальной информации:

– в электронной форме, размещенной в информационных системах или передаваемой посредством информационно-телекоммуникационных систем;

– зафиксированной на различных носителях (на бумажной, магнитной, оптической или другой основе);

4.2.3. обработка документированной конфиденциальной информации:

– размещенной в информационных системах в форме электронного документа;

– зафиксированной на различных носителях (на бумажной, магнитной, оптической или другой основе).

4.3. Требования к обработке конфиденциальной информации зависят от форм представления конфиденциальной информации и в части, не урегулированной Положением, регламентируются отдельными локальными нормативными актами.

4.4. Деятельность, связанная с обработкой конфиденциальной информации в Университете, должна включать в себя, в том числе, мероприятия по защите конфиденциальной информации от утраты и утечки.

5. Разрешительная система доступа к конфиденциальной информации

5.1. Разрешительная система доступа является частью системы правовых, организационных, технических и иных мер, принимаемых Университетом к защите конфиденциальной информации.

5.2. Разрешительная система доступа предназначена для решения следующих задач:

5.2.1. определение участников разрешительной системы доступа;

5.2.2. определение условий предоставления доступа и порядка допуска к конфиденциальной информации;

5.2.3. определение порядка работы с конфиденциальной информацией;

5.2.4. определение обязанностей лиц в рамках соблюдения разрешительной системы доступа;

5.2.5. определение степени ответственности лиц.

5.3. Принципы построения разрешительной системы доступа:

5.3.1. надежность, реализуемая принятием мер по исключению возможности несанкционированного доступа посторонних лиц к конфиденциальной информации в обычных и экстремальных условиях;

5.3.2. полнота охвата всех категорий исполнителей и всех категорий конфиденциальной информации;

5.3.3. конкретность, т.е. исключение двоякого толкования, и однозначность решения о допуске к конфиденциальной информации;

5.3.4. производственная необходимость как единственный критерий доступа исполнителя к конфиденциальной информации, а также доступа к конфиденциальной информации представителей органов власти в случаях, определяемых законодательством Российской Федерации;

5.3.5. определенность состава и компетенции должностных лиц, дающих разрешение на доступ исполнителя к конфиденциальной информации, исключение возможности бесконтрольной и несанкционированной выдачи таких разрешений;

5.3.6. строгая регламентация порядка работы с конфиденциальной информацией.

6. Участники разрешительной системы доступа в Университете

6.1. К лицам, имеющим доступ к конфиденциальной информации без

прохождения процедуры допуска в силу должностных обязанностей и ответственным за организацию разрешительной системы доступа в Университете относятся:

6.1.1. ректор Университета;

6.1.2. проректоры Университета;

6.1.3. главный бухгалтер;

6.1.4. руководители структурных подразделений.

6.2. Лица, указанные в пункте 6.1. Положения по направлениям деятельности Университета могут делегировать ответственным работникам курируемых структурных подразделений часть своих полномочий в части допуска к конфиденциальной информации в установленном в Университете порядке.

6.3. Под допускаемыми к конфиденциальной информации лицами в Университете понимаются:

6.3.1. работники Университета;

6.3.2. лица, в том числе, обучающиеся в Университете по образовательным программам, выполняющие работу или оказывающие услуги на основании гражданско-правовых договоров с Университетом;

6.3.3. иные лица (в том числе представители государственных органов).

7. Условия предоставления доступа и порядок допуска к конфиденциальной информации

7.1. Предоставление доступа к конфиденциальной информации возможно в следующих случаях:

7.1.1. конфиденциальная информация необходима для выполнения трудовых обязанностей (в том числе указанных в должностных инструкциях) допускаемых лиц из числа работников Университета;

7.1.2. конфиденциальная информация необходима для выполнения договорных обязательств допускаемыми лицами из числа указанных в подпунктах 6.3.2-6.3.4 пункта 6.3 Положения;

7.1.3. конфиденциальная информация Университета необходима для подготовки ответа уполномоченным лицом структурного подразделения Университета на запросы органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении конфиденциальной информации.

7.2. Работники Университета, которым для выполнения своих трудовых обязанностей необходимо иметь доступ к конфиденциальной информации, если такая необходимость возникла как при приеме на работу, так и в период работы в Университете, должны быть ознакомлены с настоящим Положением, перечнем конфиденциальной информации Университета, а также предупреждены об ответственности за разглашение сведений, содержащих конфиденциальную информацию.

7.3. Руководители структурных подразделений разъясняют допускаемым лицам из числа работников (в том числе поступающим на работу) особенности порядка обращения с конфиденциальной информацией, том числе с персональными данными. Инструктаж проводится в объеме Положения и других нормативных правовых и локальных нормативных актов, регламентирующих обеспечение сохранности конфиденциальной информации, в том числе персональных данных.

7.4. Допускаемые работники получают доступ в объеме, необходимом для выполнения ими своих трудовых обязанностей, с разрешения руководителя структурного подразделения и на основании прохождения процедуры допуска.

7.5. Лица из числа указанных в подпункте 6.3.2 пункта 6.3 Положения,

допускаемые к конфиденциальной информации, принимают на себя обязательства о неразглашении полученной конфиденциальной информации в соответствии с условиями соответствующих договоров.

7.6. Условия доступа представителей органов государственной власти, иных государственных органов, органов местного самоуправления или условия предоставления конфиденциальной информации Университетом по запросам указанных органов определяются в соответствии с законодательством РФ.

7.7. Процесс допуска к конфиденциальной информации направлен на исключение необоснованного расширения круга лиц, допускаемых к конфиденциальной информации, и утечки этой информации, а также доступа к ней лиц, не имеющих на то разрешения полномочных должностных лиц Университета.

7.8. Лица, которым необходимо работать с конфиденциальной информацией, могут быть допущены к конфиденциальной информации в случае, если они заявили о необходимости доступа к конфиденциальной информации, относятся к категории допускаемых лиц, прошли процедуру допуска, являющуюся составной частью разрешительной системы доступа к конфиденциальной информации Университета.

7.9. Процедуру допуска имеет право провести должностное лицо Университета, указанное в пунктах 6.1, 6.2 Положения в пределах своей компетенции.

7.10. Процедура допуска предусматривает в обязательном порядке выполнение следующих мероприятий:

7.10.1. проверка отнесения допускаемого лица к категории допускаемых лиц в соответствии с пунктом 6.3 Положения;

7.10.2. проверка выполнения условий предоставления доступа в соответствии с пунктами 7.1 – 7.7 Положения;

7.10.3. выдача разрешения на доступ к конфиденциальной информации посредством дачи соответствующего поручения в виде исполнительной надписи на документе или в виде отдельного разрешительного документа в соответствии с пунктом 7.12 настоящего Положения.

7.11. Права допускаемых лиц на доступ к конфиденциальной информации регулируются разрешениями указанных должностных лиц, оформленными в документальном (письменном или электронном) виде в отношении непосредственно подчиненных им лиц, в соответствии с пунктом 7.10 Положения.

7.12. В Университете применяются следующие способы документального оформления разрешений на доступ к конфиденциальной информации (формы разрешительных документов):

7.12.1. составление именных (должностных) списков лиц, допускаемых к той или иной конфиденциальной информации Университета, в обязательном порядке содержащих должности и фамилии лиц и категории сведений (документов), к которым они допускаются, согласно перечню Приложения, к Положению;

7.12.2. составление именных (должностных) списков лиц, допускаемых к ресурсам информационных систем, содержащих конфиденциальную информацию Университета, в обязательном порядке содержащих должности и фамилии лиц, наименование ресурсов (информации, документов, баз данных), к которым они допускаются, и прав по доступу;

7.12.3. оформление разрешения непосредственно на документе (носителе информации) в виде резолюции (поручения), адресованного конкретному лицу;

7.12.4. указание (перечисление) в организационно-распорядительных и иных документах Университета лиц (их фамилий), которые при решении конкретных производственных и иных задач должны быть допущены к определенной информации,

составляющей конфиденциальную информацию Университета.

8. Порядок работы с конфиденциальной информацией

8.1. Доступ к конфиденциальной информации предусматривает возможность ознакомления с ней и ее обработку, которая заключается в выполнении следующих действий (операций):

8.1.1. чтение (ознакомление);

8.1.2. копирование, хранение, использование, передачу, удаление (уничтожение).

8.2. Предоставление конфиденциальной информации третьим лицам, в том числе органам государственной власти, иным государственным органам, органам местного самоуправления осуществляется по распоряжению руководителя структурного подразделения.

8.3. В случае возникновения необходимости передать конфиденциальную информацию третьему лицу, должно быть получено разрешение руководителя структурного подразделения, в деятельности которого получена соответствующая конфиденциальная информация.

8.4. При передаче конфиденциальной информации контрагенту Университета разрешается использовать только способ, указанный в соглашении о неразглашении конфиденциальной информации, заключенном Университетом с соответствующим контрагентом.

9. Обязанности лиц в рамках разрешительной системы доступа

9.1. Лица, имеющие доступ к конфиденциальной информации, обязаны:

9.1.1. сохранять конфиденциальность информации, к которой они были допущены, обеспечить неразглашение сведений, составляющих конфиденциальную информацию университета, в публикациях, докладах, документации, при экспонировании на выставках, в ходе организационно-технических переговоров, служебных и неслужебных разговоров, а равно любым иным способом;

9.1.2. при работе с конфиденциальной информацией выполнять требования по защите информации, изложенные в локальных нормативных актах Университета по обеспечению информационной безопасности, в том числе сохранять в тайне свой индивидуальный пароль от компьютерной техники и сервисов, входящих в состав Единого личного кабинета, и периодически менять его;

9.1.3. при прекращении или расторжении трудового договора передать руководителю соответствующего структурного подразделения материальные носители, содержащие конфиденциальную информацию;

9.1.4. сообщать своему непосредственному руководителю или лицу, его замещающему, об утрате или недостаче документов, содержащих конфиденциальную информацию, ключей от сейфов (хранилища), печатей, удостоверений, пропусков, а также о любых иных обстоятельствах, создающих угрозу конфиденциальности информации;

9.1.5. при возникновении необходимости в передаче конфиденциальной информации по электронной почте не осуществлять передачу конфиденциальной информации с использованием иных средств, чем корпоративная электронная почта Университета;

9.1.6. при передаче конфиденциальной информации в электронной форме по корпоративной электронной почте Университета включить в исходящее письмо и в последующую переписку уведомление о конфиденциальности в следующей форме:

- на русском языке: «Это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию и предназначены исключительно для использования работниками Университета, физическим или юридическим лицом, которому они адресованы. Уведомляем Вас о том, что, если это сообщение не предназначено Вам, использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых действий на основе этой информации, не допускается. Если Вы считаете, что Вы получили это электронное сообщение по ошибке, пожалуйста, свяжитесь с отправителем и незамедлительно удалите электронное сообщение и любые вложения с компьютера. Заранее благодарим.»;
- на английском языке: «This e-mail and any attachments to it contain confidential information intended only for the use of the University staff, the individual or entity who they are addressed to. We inform you that if you are not an intended recipient of this e-mail, the use, copying, distribution of the information contained in this message, as well as the conduction of any action based on this information is not allowed. If you believe that you have received this email in error, please contact the sender and immediately delete the email and any attachments from your computer. Thank you in advance.».

9.2. Лицам, имеющим доступ к конфиденциальной информации, запрещается:

9.2.1. разглашать конфиденциальную информацию (в том числе знакомить с документами и (или) электронными документами, содержащими конфиденциальную информацию) любым лицам, кроме лиц, допущенных к конфиденциальной информации;

9.2.2. размещать конфиденциальную информацию в сети Интернет;

9.2.3. использовать конфиденциальную информацию в передачах по радио и телевидению, в публичных выступлениях;

9.2.4. снимать копии с документов и других носителей информации, содержащих конфиденциальную информацию, производить выписки из них, а равно использовать различные технические средства (фото-, видео- и звукозаписывающую аппаратуру) для регистрации сведений без разрешения руководителя соответствующего структурного подразделения;

9.2.5. осуществлять пересылку конфиденциальной информации, на личные адреса средств коммуникации (электронная почта, мессенджеры, программные средства социальных сетей и т.п.);

9.2.6. использовать без разрешения от непосредственного руководителя для хранения и обработки конфиденциальной информации личные ноутбуки, карманные персональные компьютеры, фотоаппараты, видеокамеры, электронные записные книжки, смартфоны, мобильные телефоны и другие цифровые (вычислительные) устройства, имеющие возможность ввода, хранения, накопления, приема, передачи информации[1];

9.2.7. самовольно подключать периферийные устройства[2] или устанавливать дополнительные любые программные средства, копировать конфиденциальную информацию на личные флеш-карты и иные устройства хранения информации;

9.2.8. использовать для хранения конфиденциальной информации облачные сервисы, за исключением сервисов, контролируемых Университетом.

9.3. Лица, имеющие доступ к конфиденциальной информации, обязаны:

---

[1]Исключения из этого правила допускаются исключительно для научно-педагогических работников по решению руководителя структурного подразделения, в котором работает работник.

[2] Под периферийным устройством необходимо понимать внешние по отношению к системному блоку компьютера устройства (USB-флеш, внешний CD-ROM, внешний жесткий диск, VPN-ключ, e-token).

9.3.1. не создавать копии (в том числе электронные) конфиденциальной информации (в том числе на отделяемые (внешние) носители информации) без получения предварительного согласия руководителя соответствующего структурного подразделения;

9.3.2. определять количество экземпляров документов (в том числе электронных), содержащих конфиденциальную информацию, в строгом соответствии с действительной необходимостью;

9.3.3. использовать при работе с конфиденциальной информацией Университета, контрагента Университета только средства вычислительной техники (стационарные компьютеры, мобильные устройства), оснащенные средствами защиты, достаточными для обеспечения информационной безопасности в соответствии с требованиями локальных актов, определяющих политику информационной безопасности Университета;

9.3.4. прекратить обработку конфиденциальной информации на компьютерной технике при обнаружении в последней неисправностей, вирусов, шпионских программ, программ-майнеров, других вредоносных программ и сообщить о выявленных неисправностях своему непосредственному руководителю (или лицу, его замещающему).

9.4. Ответственными за обеспечение режима конфиденциальности информации в структурных подразделениях Университета являются руководители соответствующих структурных подразделений.

9.5. При получении Университетом информации, в отношении которой требуется установление режима конфиденциальности, руководитель структурного подразделения, в деятельности которого получена соответствующая информация, обеспечивает принятие всех необходимых мер по установлению и поддержанию режима конфиденциальности информации, указанных в Положении. Если конфиденциальная информация была получена в деятельности нескольких подразделений, меры по установлению и поддержанию режима конфиденциальности информации применяются совместно руководителями указанных подразделений.

9.6. В целях поддержания режима конфиденциальности информации руководитель структурного подразделения в том числе:

9.6.1. обеспечивает учет лиц, получивших доступ к конфиденциальной информации, и (или) лиц, которым такая информация была предоставлена или передана;

9.6.2. уведомляет работника, доступ которого к конфиденциальной информации необходим для выполнения им своих трудовых обязанностей, о конфиденциальном характере раскрываемой работнику информации, обладателями которой являются Университет или его контрагенты;

9.6.3. контролирует факт ознакомления под подпись работника с Положением и иными локальными нормативными актами, направленными на обеспечение конфиденциальности информации в Университете и с мерами ответственности за их нарушение;

9.6.4. создает работнику необходимые условия для соблюдения им установленного Университетом режима конфиденциальной информации;

9.6.5. обеспечивает при заключении с контрагентами Университета, в том числе с лицами, выполняющими работы (оказывающими услуги) в пользу Университета на основании гражданско-правовых договоров, наличие в соответствующих договорах условий о неразглашении конфиденциальной информации;

9.6.6. исполняет иные обязанности, предусмотренные Положением.

9.7. Если информация, в отношении которой целесообразно установление режима конфиденциальности информации, получена в ходе выполнения работ по договору или реализации соглашения, в целях определения конкретных сведений, подлежащих охране, необходимых мер по защите информации, а также для урегулирования иных вопросов, руководитель подразделения, ответственный за исполнение договора (соглашения) со стороны Университета, обеспечивает включение в соответствующий договор (соглашение) положений, определяющих взаимные обязательства и ответственность сторон за ее сохранность.

9.8. В случае, если обладателем конфиденциальной информации является контрагент Университета, в договоре с которым предусмотрена обязанность Университета уведомить контрагента о факте предоставления информации в ответ на основанное на законе требование органа государственной власти, иного государственного органа, органа местного самоуправления, руководитель структурного подразделения Университета, ответственный за исполнение договора, обеспечивает направление контрагенту соответствующего уведомления в случаях, когда данные действия не будут являться нарушением требований применимого законодательства.

10. Ответственность за нарушение режима конфиденциальности информации

10.1. Ответственность за нарушение режима конфиденциальности основывается на принципе персональной ответственности, который заключается в том, что каждое лицо, разрешающее доступ или получившее доступ к конфиденциальной информации должно лично отвечать за свою деятельность, включая любые действия с конфиденциальной информацией и возможные нарушения по обеспечению ее безопасности, т.е. какие-либо случайные или умышленные действия, которые приводят или могут привести к несанкционированной утечке или утрате конфиденциальной информации.

10.2. Лица, разгласившие конфиденциальную информацию, или иным образом нарушившие установленную Положением разрешительную систему доступа, работы и хранения конфиденциальной информации, несут дисциплинарную, гражданско-правовую и иную ответственность в установленном законодательством Российской Федерации порядке.

10.3. Нарушением режима конфиденциальности информации признаются, в том числе:

10.3.1. разглашение конфиденциальной информации;

10.3.2. неправомерное использование конфиденциальной информации;

10.3.3. несанкционированный доступ к конфиденциальной информации;

10.3.4. утрата документов и иных материальных носителей, содержащих конфиденциальную информацию;

10.3.5. неправомерное уничтожение документов, содержащих конфиденциальную информацию;

10.3.6. нарушение требований хранения документов, содержащих конфиденциальную информацию;

10.3.7. другие нарушения требований законодательства и настоящего Положения.

Приложение
к Положению о защите конфиденциальной информации
ФГБОУ ВО КубГМУ Минздрава России

Перечень конфиденциальной информации
ФГБОУ ВО КубГМУ Минздрава России

№	Направления деятельности	Лица, уполномоченные на распоряжение конфиденциальной информацией	Основные категории конфиденциальной информации
1	По всем направлениям деятельности	Руководители структурных подразделений (участники деятельности)	1. информация о хозяйственно-финансовых отношениях с деловыми партнерами (в том числе условия договорных отношений с ними), о проведении переговоров, переписке с ними, в рамках условий о конфиденциальности, определённых непосредственно сторонами отношений; 2. информация, составляющая электронную базу Университета, содержащая сведения об обучающихся, работниках, деловых партнерах Университета; 3. не являющаяся общедоступной информация о деятельности Университета; 4. текущие оперативные сведения о технико-экономических показателях деятельности Университета, обязанность по раскрытию которых не предусмотрена законодательством; 5. условия сделок, за исключением существенных, которые имеют гласный характер, т. е. подлежат обязательному доведению до сведения любых заинтересованных лиц; 6. содержание работ, проводимых на основании договоров с контрагентами, касающихся научно-исследовательских, опытно-конструкторских и технологических работ, а равно иных работ, в результате которых возможно создание результатов интеллектуальной деятельности; 7. сведения о контрагентах Университета (в т.ч. состояние расчетов с контрагентами, включая активы контрагентов; состав поручений контрагентов); которые не содержатся в открытых источниках (справочниках, каталогах и др.) или переданы в Университет указанными лицами на доверительной основе (в том числе адреса, телефоны, сведения об имущественных правах, аффилированных лицах, деловых связях, финансовом и экономическом состоянии и т.п.), а также персональная информация о работниках контрагентов; 8. сведения о подготовке, принятии и исполнении решений руководства по вопросам его деятельности, развития, а также по иным организационным и научно-техническим вопросам; 9. идентификаторы и пароли, используемые сотрудниками Университета для доступа в служебные помещения, к информации в электронном виде; 10. информация, полученная Университетов в рамках исполнения договора (контракта) и определенная раскрывающей стороной как конфиденциальная, за исключением информации,

			подлежащей обнародованию и предоставлению третьим лицам во исполнение требований действующего законодательства; 11. сведения о совещаниях, проводимых в Университете, и содержание обсуждаемой на таких совещаниях информации, при условии, что до начала совещания или во время проведения совещания было сделано предупреждение в любой форме о конфиденциальности такого совещания; 12. информация о личных отношениях работников как между собой, так и с руководством, сведения о возможных противоречиях, конфликтах внутри коллектива; 13. сведения о необъявленных официально планах вывода на рынок новых результатов НИР, а также образовательных услуг и программ; 14. сведения о результатах интеллектуальной деятельности, исключительное право на которые принадлежит Университету, до получения ими правовой охраны / защиты; 15. отчетные документы по результатам внутренних проверок (в т.ч. документы по учету нарушений студентами); 16. информация, составляющая коммерческую тайну Университета.
2	Деятельность по общему делопроизводству (то есть за исключением кадрового делопроизводства)	Сектор делопроизводства: руководитель и ответственные сотрудники	1. оперативные (текущие) документы общего делопроизводства: внутренние (организационные, распорядительные, информационно-справочные и др.); 2. входящая (за исключением входящих рекламных предложений) и исходящая корреспонденция (в том числе в электронном виде).
3	Деятельность по ведению архива	Начальник управления кадров	1. информация о системе архивного хранения и использования архивных документов Университета; 2. архивные документы кадрового делопроизводства; 3. архивные научно-технические документы (отчеты по НИР)
4	Деятельность по обеспечению безопасности	Начальник управления по безопасности	1. Сведения о порядке и состоянии организации безопасности и системе охраны, пропускном режиме, противопожарной безопасности, систем сигнализации (охранной и АПС) и т.п. 2. Переписка с правоохранительными органами, структурными подразделениями МЧС России, органами ГО ЧС и ПБ. 3. Материалы расследований и разбирательств. 4. Документы по учету нарушений. 5. Документы внешнего и внутреннего аудита. 6. Материалы по профилактике распространения и потребления ПАВ.
5	Закупочная деятельность	Начальник Отдел государственного заказа и материально-технического снабжения	1.Сведения о готовящихся торгах и документация о таких торгах до их объявления.

6	Деятельность по связям с общественностью	Начальник организационного отдела, ответственные работники	1. информация, отмеченная грифом «для служебного пользования»; 2. сведения о планах Университета в отношении формирования публичной информационной политики
7	Деятельность по подбору персонала и кадровая работа	Начальник управления кадров	1. сведения о размере заработной платы; сведения о принятии решений, касающихся материального стимулирования работников, в том числе о процедуре их согласования; 2. положения трудовых договоров (контрактов), заключаемых с работниками, за исключением сведений, которые не могут относиться к конфиденциальной информации в соответствии с законодательством Российской Федерации; 3. система организации труда, за исключением информации, подлежащей обнародованию и предоставлению третьим лицам во исполнение требований действующего законодательства
8	Финансовая и бухгалтерская деятельность	Главный бухгалтер Начальник планово-финансового управления	1. Финансовая информация, имеющая коммерческую ценность, не содержащаяся в учредительных и иных документах, находящихся в публичном доступе, а также относящаяся к категории ограниченного доступа, в том числе:
			- персональная информация физических лиц; - образцы подписей физических лиц; - документы, содержащие сведения о получаемых и предлагаемых предложениях; - деловая переписка; - протоколы закрытых совещаний;
			- информация, содержащаяся в регистрах бухгалтерского учета и внутренней бухгалтерской отчетности; - данные налогового учета и налоговой отчетности; - сведения об исполнении договоров, контрактов и соглашений; - данные первичных учетных документов; - персональная информация физических лиц;
			- штатная расстановка с указанием ФИО и оплаты труда работников; - сведения, касающиеся предмета договоров на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, а равно договоров о создании результатов интеллектуальной деятельности, хода их исполнения и полученных результатов, если иное не предусмотрено договорами; - персональная информация физических лиц;
9	Деятельность по цифровизации процессов Университета и обеспечению информационной безопасности	Начальник отдела информационных технологий	1. Информация по параметрам доступа (включая имена пользователей и пароли) к разрабатываемым и поддерживаемым управлением информационным системам Университета (ИСУ) 2. Бизнес схемы, описывающие реализованные или планируемые к реализации процессы в ИСУ 3. Технические задания на модернизацию существующих и создание новых ИСУ
			Реквизиты административного доступа к серверному, сетевому оборудованию, системам хранения данных, системам управления средой виртуализации и ИСУ

			Сведения о производственно-технологических процессах, схемы и методики, дающие преимущество Университету.
			1.Реквизиты административного доступа к системам защиты информации. 2.Сведения, содержащиеся в материалах, описывающих следующие направления обеспечения информационной безопасности, и которые могут быть использованы в дальнейшем для противоправных действий по нанесению ущерба Университету: – о проектных решениях по обеспечению защиты информации при разработке, модернизации и эксплуатации корпоративных информационных систем; – о результатах комплексных проверок эффективности системы защиты информации корпоративных информационных систем до утверждения акта (заключения) по проверке; – о результатах анализа проведенных расследований инцидентов информационной безопасности.
10	Деятельность по правовому сопровождению	Начальник юридического отдела	1. персональная информация физических лиц; 2. информация, ставшая известной при подготовке материалов по результатам рассмотрения актов органов власти и служебных проверок, переписка с правоохранительными органами, материалы расследований и разбирательств; 3. информация об Университете, ставшая известной в процессе рассмотрения претензий, жалоб, обращений, дисциплинарных производств, подготовки дела к судебному разбирательству, в процессе судебного разбирательства, по итогам судебного разбирательства (за исключением общедоступной информации); 4. правовые позиции юридического отдела по правовым вопросам, если они не были сделаны Университетом общедоступными.
11	Деятельность по созданию, оформлению, получению правовой охраны, коммерциализации объектов интеллектуальной собственности	Начальник научно-организационного управления	1. информация о секретах производства (ноу-хау); 2. сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них; 3. сведения о предмете научно-исследовательских работ, опытно-конструкторских и технологических работ; 4. информация о планируемых к разработке объектов интеллектуальной собственности, 5. условия договоров на проведение клинических исследований, выполнение научно-исследовательских, опытно-конструкторских и технологических работ, соглашений о научном сотрудничестве, обозначенные сторонами договоров и соглашений конфиденциальными; 6. иная информация, отнесенная Университетом к коммерческой тайне.