ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ВЛАДИМИРСКОЙ ОБЛАСТИ

«РЕГИОНАЛЬНЫЙ ИНФОРМАЦИОННО – АНАЛИТИЧЕСКИЙ ЦЕНТР ОЦЕНКИ КАЧЕСТВА ОБРАЗОВАНИЯ»

П Р И К А З

«22» сентября 2023 г. № 674/02-04

Об утверждении перечня сведений конфиденциального характера и Положения о работе с конфиденциальной информацией в ГБУ ВО РИАЦОКО

В соответствии с 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» в целях организации работы с конфиденциальной информацией в государственном бюджетном учреждении Владимирской области «Региональный информационно – аналитический центр оценки качества образования» (далее – ГБУ ВО РИАЦОКО) п р и к а з ы в а ю:

1. Утвердить перечень сведений конфиденциального характера в ГБУ ВО РИАЦОКО (далее – Перечень) согласно Приложению № 1.
2. Утвердить положение о работе с конфиденциальной информацией в ГБУ ВО РИАЦОКО (далее – Положение КИ) согласно Приложению № 2.
3. Заведующему отдела информационно-технического обеспечения процедур оценки качества образования и защиты информации Р.С.Дадаеву довести Перечень и Положение КИ до сведения всех сотрудников ГБУ ВО РИАЦОКО в срок до 03.10.2023 г. под роспись в листе ознакомления.
4. Настоящий приказ вступает в силу с момента его принятия.
5. Контроль за исполнением настоящего приказа возложить на заместителя директора В.В.Данилова

Директор С.И.Мансурова

Приложение № 1
к приказу ГБУ ВО РИАЦОКО
от «22» сентября 2023 г. № 678/2023

ПЕРЕЧЕНЬ
сведений конфиденциального характера в ГБУ ВО РИАЦОКО

№ п/п	Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
1.	Персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому лицу).	Статья 7 Федерального закона от 27.06.2006 года №152-ФЗ «О персональных данных».
2.	Сведения, ставшие известными в связи с исполнением должностных обязанностей, в том числе сведения, касающиеся частной жизни и здоровья граждан или затрагивающие их честь и достоинство.	Пункт 6 статьи 12 Федерального закона от 02.03.2007 года №25-ФЗ «О муниципальной службе в Российской Федерации».
3.	Сведения о личной и семейной тайне. Сведения, раскрывающие тайну переписки, телефонных переговоров, почтовых и иных сообщений.	Статья 23 Конституции Российской Федерации, принятой всенародным голосованием 12 декабря 1993 года.
4.	Сведения, содержащиеся в проектах документов (или) прилагаемых к ним материалах на любом носителе информации до официальной публикации.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».
5.	Сведения, содержащиеся в материалах служебных расследований (проверок), до издания соответствующих распорядительных документов.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».
6.	Сведения о системах защиты информации (средства, методы и способы защиты информации, реквизиты доступа, модели угроз, технические паспорта информационных систем, матрицы доступа, пароли, ключи электронной подписи, процедуры доступа к информационным системам и ресурсам). Сведения об оценке эффективности защиты информации.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации». Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
7.	Сведения об информационно-	Пункт 3 статьи 6 Федерального

	телекоммуникационных сетях и каналах связи, компьютерных сетях, программном обеспечении, системах и средствах охранно-тревожной, пожарной сигнализации и видеонаблюдения.	закона От 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».

Приложение № 2
к приказу ГБУ ВО РИАЦОКО
от «22» сентября 2023 г.№ 644/22-04

Положение о работе с конфиденциальной информацией в государственном бюджетном учреждении Владимирской области «Региональный информационно – аналитический центр оценки качества образования»

1. Нормативная база

Положение о сведениях, составляющих конфиденциальную информацию (далее - Положение) в государственном бюджетном учреждении Владимирской области «Региональный информационно-аналитический центр оценки качества образования» (далее - ГБУ ВО РИАЦОКО), разработано на основе:
- Гражданского кодекса Российской Федерации;
- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных";
- Указа Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Политики ГБУ ВО РИАЦОКО в отношении обработки защищаемой информации, не содержащей сведения, составляющей государственную тайну;
- Концепции информационной безопасности информационной системы ГБУ ВО РИАЦОКО;
-Правил работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходимых для выполнения ими служебных (трудовых) обязанностей в ГБУ ВО РИАЦОКО;
-Инструкции ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных;
-Порядка уничтожения персональных данных при достижении целей обработки и (или) при наступлении законных оснований;
-Правил осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;
- Инструкции по работе с инцидентами информационной безопасности;
- Инструкции по работе администратора информационной безопасности;
-Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну в государственном бюджетном учреждении Владимирской области «Региональный информационно-аналитический центр оценки качества образования».

2. Общие положения

2.1. Положение о работе с конфиденциальной информацией (далее - КИ) при ее обработке в учреждении (далее - Положение) относится к основополагающим документам, определяющим общие принципы организации работ по информационной безопасности КИ.

2.2. Организация и проведение работ по обеспечению безопасности информации, содержащей КИ, на объектах информатизации ГБУ ВО РИАЦОКО проводится на основании законодательных и нормативных актов Российской Федерации в области защиты информации и настоящего Положения.

2.3. Требования настоящего Положения являются обязательными для исполнения в ГБУ ВО РИАЦОКО.

2.4. Положение определяет порядок организации и проведения работ по защите информации, содержащей КИ, на объектах информатизации и на бумажных носителях ГБУ ВО РИАЦОКО как в период их создания, так и в процессе повседневной эксплуатации.

2.5. Принимаемые меры по защите информации на объектах информатизации ГБУ ВО РИАЦОКО должны обеспечивать выполнение действующих требований и норм по защите информации.

2.6. Разработка мер и обеспечение защиты информации на объектах информатизации осуществляются отделом информационно-технического обеспечения процедур оценки качества образования и защиты информации ГБУ ВО РИАЦОКО.

2.7. Разработка мер защиты информации может осуществляться также сторонними организациями, имеющими лицензии ФСТЭК России и ФСБ России на право проведения соответствующих работ.

2.8. Согласование планируемых мер, контроль выполнения работ на местах, соответствия принятых мер и проводимых мероприятий по защите информации действующим требованиям и нормам производит отдел информационно-технического обеспечения процедур оценки качества образования и защиты информации ГБУ ВО РИАЦОКО.

2.9. Объекты информатизации организации должны соответствовать требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России.

2.10. Защита информации организуется в соответствии с действующими нормативными документами ФСТЭК России.

2.11. Ответственность за общее состояние и организацию работ по созданию и эксплуатации объектов информатизации возлагается на заведующего отделом информационно-технического обеспечения процедур оценки качества образования и защиты информации ГБУ ВО РИАЦОКО.

2.12. Ответственность за обеспечение требований по защите информации, циркулирующей на объектах информатизации, возлагается на заведующих структурных подразделений организации, эксплуатирующих эти объекты.

2.13. В Положении используются следующие понятия:

2.13.1. **Информация** - сведения (сообщения, данные) независимо от формы их представления (текстовая, числовая, графическая, аудио, видео, электронная), в том числе:

2.13.2. **Данные** - сведения, зафиксированные в какой-либо форме;

2.13.3. **Сообщения** - сведения в какой-либо форме, передаваемые между участниками информационного взаимодействия;

2.13.4. **Документированная информация** - информация, зафиксированная на материальном носителе (в том числе на бумажном) путем документирования с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

2.13.5. **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;

2.13.6. **Конфиденциальность информации** - требование не разглашать информацию третьим лицам без согласия ее обладателя, обязательное для выполнения лицом, получившим доступ к определенной информации;

2.13.7. **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 ГБУ ВО

РИАЦОКО и его работников, и в отношении которой в ГБУ ВО РИАЦОКО введен режим конфиденциальности информации.

Возможными формами представления конфиденциальной информации являются:

речевая информация - (информация, представленная в виде информативных акустических сигналов, которая озвучивается в том числе устно на встречах или совещаниях) и **звуковая информация** (информация, представленная в виде информативных акустических сигналов, которая озвучивается посредством звуковоспроизводящих устройств);

2.13.8. **Информация в электронной форме** - информация, размещаемая в информационных системах (обрабатывается на средствах вычислительной техники при помощи информационных технологий, представленная в виде информационных массивов, отдельных файлов и баз данных) и/или передаваемая посредством информационно-телекоммуникационных систем (по каналам связи, локальным или глобальным вычислительным сетям);

2.13.9. **Недокументированная информация**, зафиксированная на различных носителях (на бумажной, магнитной, оптической или другой основе);

2.13.10. **Документированная информация**, зафиксированная на различных носителях (на бумажной, магнитной, оптической или другой основе);

2.13.11. Документированная информация, размещаемая в информационных системах, в форме электронного документа.

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

2.13.13. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.13.14. **Иные сведения конфиденциального характера ГБУ ВО РИАЦОКО** - сведения в любой объективной форме, создаваемые и используемые работниками ГБУ ВО РИАЦОКО, а также физическими лицами - исполнителями по гражданско-правовым договорам, при исполнении трудовых(функциональных) обязанностей;

2.13.15. **Обладатель информации** - юридическое лицо ГБУ ВО РИАЦОКО 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;

2.13.16. **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;

2.13.17. **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);

2.13.18. **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 ГБУ ВО РИАЦОКО 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.

2.13.19. **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;

2.13.20. **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;

2.13.21. **Утрата конфиденциальной информации** - наносящее ущерб ГБУ ВО РИАЦОКО 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;

2.13.22. **Утечка конфиденциальной информации** - неправомерный (неразрешенный) выход такой информации за пределы защищаемой зоны ее функционирования в ГБУ ВО РИАЦОКО 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;

2.13.23. **Контролируемая зона (КЗ)** - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

2.13.24. **Несанкционированный доступ (несанкционированные действия) (НСД)** - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим техническим характеристикам и функциональному предназначению.

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

2.13.26. **Средства вычислительной техники (СВТ)** - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

2.13.27. **Побочные электромагнитные излучения и наводки (ПЭМИН)** - электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

2.13.28. **Система защиты информации** - совокупность органов и (или) исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

2.13.29. **Объекты информатизации** - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

2.13.30. **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;

2.13.31. **Лицо, привлекаемое в ГБУ ВО РИАЦОКО** - физическое лицо и лицо вступившее в трудовые или гражданско-правовые отношения с ГБУ ВО РИАЦОКО.

3. Порядок определения сведений конфиденциального характера в ГБУ ВО РИАЦОКО

3.1. К защищаемой КИ в ГБУ ВО РИАЦОКО относится:

№ п/п	Сведения, отнесенные к категории ограниченного доступа	Основания отнесения сведений к категории ограниченного доступа
1.	Персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому лицу).	Статья 7 Федерального закона от 27.06.2006 года №152-ФЗ «О персональных данных».
2.	Сведения, ставшие известными в связи с исполнением должностных обязанностей, в том числе сведения, касающиеся частной жизни и здоровья граждан или затрагивающие их честь и достоинство.	Пункт 6 статьи 12 Федерального закона от 02.03.2007 года №25-ФЗ «О муниципальной службе в Российской Федерации». Пункт 5 статьи 9 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».
3.	Сведения о личной и семейной тайне. Сведения, раскрывающие тайну переписки, телефонных переговоров, почтовых и иных сообщений.	Статья 23 Конституции Российской Федерации, принятой всенародным голосованием 12 декабря 1993 года.
4.	Сведения, содержащиеся в проектах документов (или) прилагаемых к ним материалах на любом носителе информации, до официальной публикации.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».
5.	Сведения, содержащиеся в материалах служебных расследований (проверок), до издания соответствующих распорядительных документов.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».
6.	Сведения о системах защиты информации (средства, методы и способы защиты информации, реквизиты доступа, модели угроз, технические паспорта информационных систем, матрицы	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации,

	доступа, пароли, ключи электронной подписи, процедуры доступа к информационным системам и ресурсам). Сведения об оценке эффективности защиты информации.	информационных технологиях и о защите информации». Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
7.	Сведения об информационно-телекоммуникационных сетях и каналах связи, компьютерных сетях, системах и средствах охранно-тревожной, пожарной сигнализации и видеонаблюдения.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».

3.2. Защищаемая информация организации может быть представлена:

- на бумажных носителях в виде отдельных документов или дел с документами;
- на машинных носителях в виде файлов, массивов, баз данных, библиотек и пр.;
- в виде речевой информации, при проведении совещаний, переговоров и пр.

3.3. С целью определения технических средств и систем, с помощью которых обрабатывается информация, содержащая КИ, а также помещений, где проводятся мероприятия с использованием такой информации, отделом информационно-технического обеспечения процедур оценки качества образования и защиты информации ГБУ ВО РИАЦОКО утверждается перечень технических средств и защищаемых помещений.

4. Основные цели и задачи защиты конфиденциальной информации на объектах ГБУ ВО РИАЦОКО

4.1. Положение о работе с КИ в ГБУ ВО РИАЦОКО регулирует отношения, связанные с обработкой КИ, создаваемой и/или используемой в деятельности ГБУ ВО РИАЦОКО, в отношении которой ГБУ ВО РИАЦОКО является обладателем информации.

4.2. Для достижения цели в Положении определяются способы решения следующих задач:

4.3. Определение конфиденциальной информации ГБУ ВО РИАЦОКО;

4.4. Определение общих требований по обработке конфиденциальной информации;

4.5. Определение разрешительной системы доступа к конфиденциальной информации как основы ограничения доступа к конфиденциальной информации.

4.6. Основными принципами, которыми руководствуется ГБУ ВО РИАЦОКО в вопросах ограничения доступа к конфиденциальной информации, являются:

4.6.1. Законность ограничения доступа - заключается в выполнении требований законодательства при отнесении информации (сведений, данных) к конфиденциальной информации. При этом учитываются нормы, предписывающие ограничения на доступ к этим сведениям, как и запрещающие такие ограничения;

4.6.2. Обоснованность ограничения доступа - заключается в установлении путем экспертной оценки работниками ГБУ ВО РИАЦОКО отнесения информации к отдельным видам сведений, исходя из законных интересов ГБУ ВО РИАЦОКО и в соответствии с принятыми в ГБУ ВО РИАЦОКО локальными нормативными актами;

4.6.3. Своевременность ограничения доступа - заключается в установлении ограничений на разглашение и (или) распространение сведений с момента их получения (разработки) или заблаговременно.

4.7. 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 ГБУ ВО РИАЦОКО разрешительной системы доступа к КИ допускаемых лиц (далее - разрешительная система доступа).

5. Условия предоставления доступа и порядок допуска к конфиденциальной информации

5.1. Предоставление доступа к КИ возможно в следующих случаях:

5.1.1. КИ необходима для выполнения трудовых обязанностей (в том числе указанных в должностных инструкциях) допускаемых лиц из числа сотрудников ГБУ ВО РИАЦОКО;

5.1.2. КИ ГБУ ВО РИАЦОКО необходима для подготовки ответа уполномоченным лицом структурного подразделения ГБУ ВО РИАЦОКО на запросы органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении конфиденциальной информации.

5.2. Сотрудники ГБУ ВО РИАЦОКО, которым для выполнения своих трудовых обязанностей необходимо иметь доступ к КИ, если такая необходимость возникла как при приеме на работу, так и в период работы в ГБУ ВО РИАЦОКО, должны быть ознакомлены с настоящим Положением, перечнем КИ ГБУ ВО РИАЦОКО, предупреждены об ответственности за разглашение сведений, содержащих КИ, и должны дать письменное обязательство о неразглашении указанных сведений в соответствии с примерной формой, приведенной в Приложении №1 к Положению. Указанные формы могут изменяться либо корректироваться подразделением по согласованию с директором или лицом его замещающим в ГБУ ВО РИАЦОКО.

5.3. Заведующие структурными подразделениями ГБУ ВО РИАЦОКО разъясняют допускаемым лицам из числа сотрудников(в том числе поступающих на работу) особенности порядка обращения с КИ, том числе с персональными данными. Инструктаж проводится в объеме Положения или других нормативных правовых и локальных нормативных актов, регламентирующих обеспечение сохранности КИ, в том числе персональных данных.

5.4. Допускаемые сотрудники получают доступ в объеме, необходимом для выполнения ими трудовых обязанностей, по ходатайству с разрешения руководителя структурным подразделением и на основании прохождения процедуры допуска.

5.5. Лица, допускаемые к КИ, принимают на себя обязательства о неразглашении полученной КИ по форме, которая приведена в Приложении №1 к Положению.

5.6. Условия доступа представителей органов государственной власти, иных государственных органов, органов местного самоуправления или условия предоставления КИ ГБУ ВО РИАЦОКО по запросам указанных органов определяются в соответствии с законодательством РФ.

5.7. Процесс допуска к КИ направлен на исключение необоснованного расширения круга лиц, допускаемых к КИ, и утечки этой информации, а также доступа к ней лиц, не имеющих на то разрешения полномочных должностных лиц ГБУ ВО РИАЦОКО.

5.8. Лица, которым необходимо работать с КИ, могут быть допущены к КИ в случае, если они заявили о необходимости доступа к КИ, относятся к категории допускаемых лиц, прошли процедуру допуска, являющуюся составной частью разрешительной системы доступа к КИ ГБУ ВО РИАЦОКО.

5.9. Процедуру допуска имеет право провести должностное лицо ГБУ ВО РИАЦОКО, в пределах своей компетенции.

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

5.10.1. Проверка отнесения допускаемого лица к категории допускаемых лиц в соответствии с Положением;

5.10.2. Проверка выполнения условий предоставления доступа в соответствии с Положением;

5.10.3. Выдача разрешения на доступ к КИ;

5.11. Права допускаемых лиц на доступ к КИ регулируются разрешениями должностных лиц, оформленными в документальном (письменном или электронном) виде в отношении непосредственно подчиненных им лиц.

6. Общие требования по обработке конфиденциальной информации

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

6.2. В ГБУ ВО РИАЦОКО, в зависимости от форм представления КИ, регламентируются следующие направления обработки КИ:

6.2.1. Обработка речевой и/или звуковой КИ;

6.2.2. Обработка недокументированной КИ:

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

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

6.2.3. Обработка документированной КИ:

– размещенной в информационных системах в форме электронного документа;

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

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

6.4. Деятельность, связанная с обработкой конфиденциальной информации в ГБУ ВО РИАЦОКО, должна включать в себя, в том числе, мероприятия по защите КИ от утраты и утечки.

7. Порядок работы с конфиденциальной информацией

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

7.1.1. Чтение (ознакомление);

7.1.2. Копирование, хранение, использование, передачу, удаление (уничтожение).

7.2. Лица, имеющие доступ к КИ, обязаны:

7.2.1. Сохранять КИ, к которой они были допущены, обеспечить неразглашение сведений, составляющих КИ ГБУ ВО РИАЦОКО, в публикациях, докладах, документации, в ходе организационно-технических переговоров, служебных и неслужебных разговоров;

7.2.2. При работе с КИ выполнять требования по защите информации, изложенные в локальных нормативных актах ГБУ ВО РИАЦОКО по обеспечению информационной безопасности, в том числе сохранять в тайне свой индивидуальный пароль от компьютерной техники;

7.2.3. При прекращении или расторжении трудового договора передать заведующему соответствующего структурного подразделения материальные носители, содержащие КИ;

7.2.4. 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;

7.2.5. При возникновении необходимости в передаче КИ в электронном виде не осуществлять передачу КИ с использованием иных средств, чем по защищенному каналу связи (криптографическая сеть 4479, 3831, 1372) ГБУ ВО РИАЦОКО (если иное не предусмотрено в отдельном соглашении или обязательстве о неразглашении);

7.2.6. Передача, пересылка, рассылка КИ по электронной почте запрещена;

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

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

7.3.2. Размещать КИ в сети Интернет;

7.3.3. Использовать КИ в передачах по радио и телевидению, в публичных выступлениях;

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

7.3.5. Осуществлять пересылку КИ: на личные адреса средств коммуникации (электронная почта, мессенджеры, программные средства социальных сетей и т.п.);

7.3.6. Использовать без разрешения от непосредственного руководителя, 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;

7.3.7. Самовольно подключать периферийные устройства или устанавливать дополнительные любые программные средства, копировать конфиденциальную информацию на личные флэш-карты и иные устройства хранения информации;

7.3.8. Использовать для хранения КИ облачные сервисы, за исключением сервисов, контролируемых ГБУ ВО РИАЦОКО.

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

7.4.1. Не создавать копии (в том числе электронные) КИ (в том числе на отделяемые (внешние) носители информации) без получения предварительного согласия руководителя структурным подразделением;

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

7.4.3. Использовать при работе с КИ ГБУ ВО РИАЦОКО, контрагента ГБУ ВО РИАЦОКО 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 ГБУ ВО РИАЦОКО;

7.4.4. Прекратить обработку КИ на компьютерной технике при обнаружении в последней неисправностей, вирусов, шпионских программ, программ-майнеров, других вредоносных программ и сообщить о выявленных неисправностях своему непосредственному руководителю и/или лицу, его замещающему, и администратору информационной безопасности.,

8. Ответственность за нарушение режима конфиденциальности информации

8.1. Ответственность должностных лиц за обеспечение защиты конфиденциальной информации на объекте информатизации.

8.1.1. Ответственный за организацию обработки персональных данных (назначенный приказом ГБУ ВО РИАЦОКО) несет ответственность за общую организацию работ по защите информации на объектах информатизации и на бумажных носителях.

8.1.2. Администратор информационной безопасности ГБУ ВО РИАЦОКО (назначенный приказом ГБУ ВО РИАЦОКО) несет ответственность за:

- руководство и координацию работ по защите информации на объектах информатизации;
- организацию выполнения требований по защите информации на объекте информатизации;
- обоснованность необходимости создания СЗКИ объекта информатизации;
- разработку организационно-распорядительных документов по защите информации на объектах информатизации;
- организацию разработки технического задания на создание СЗКИ, организацию подготовки проектов договоров со сторонними организациями на выполнение работ по защите информации на объектах информатизации;
- организацию контроля состояния СЗКИ объекта информатизации, соблюдения работниками установленных норм и требований по защите информации;
- сопровождение СЗИ от несанкционированного доступа;
- настройку и сопровождение в процессе эксплуатации подсистемы управления доступом;
- проверку состояния используемых СЗИ от несанкционированного доступа, правильности их настройки;
- организацию разграничения доступа;
- учет и контроль состава и полномочий пользователей;
- учет, хранение, прием и выдачу персональных идентификаторов и ключевых носителей ответственным исполнителям;
- контроль учета, создания, хранения и использования резервных и архивных копий массивов данных;
- выбор типа и версии серверных и клиентских операционных систем, установку, настройку, сопровождение операционных систем серверов;
- обновление справочного и антивирусного программного обеспечения;
- организацию настройки аппаратной и программной составляющей серверного, коммутационного, телекоммуникационного оборудования, средств аппаратной безопасности сегментов, сетевого периферийного оборудования;
- регистрацию пользователей и предоставление им прав доступа к сетевым информационным ресурсам, регистрацию компьютеров в сети;
- реализацию адресной и маршрутной политики сети;
- реализацию политики антивирусной защиты;
- обеспечение работоспособности структурированной кабельной сети;
- архивирование, резервное копирование информации;
- ведение аудита системных событий и безопасности;
- оперативное управление работой сети;
- контроль физической сохранности средств и оборудования сети.

8.1.3. Сотрудники ГБУ ВО РИАЦОКО, эксплуатирующие объект информатизации и бумажные носители, несут ответственность за:

- выполнение требований по защите информации на объекте информатизации;
- ведение необходимой документации объекта информатизации;
- правильность определения пользователям своего подразделения необходимости и прав доступа к защищаемым информационным ресурсам.

8.2. Ответственными за обеспечение режима конфиденциальности информации в структурных подразделениях ГБУ ВО РИАЦОКО являются руководители структурных

подразделений.

8.2.1 При получении ГБУ ВО РИАЦОКО 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 КИ была получена в результате деятельности нескольких подразделений, меры по установлению и поддержанию режима конфиденциальности информации принимаются совместно с руководителем структурного подразделения, а также с другими лицами, имеющими доступ к этой информации.

8.2.2. В целях поддержания режима КИ руководитель структурного подразделения в том числе:

– уведомляет работника, доступ которого к КИ необходим для выполнения им своих трудовых обязанностей, о конфиденциальном характере раскрываемой работнику информации, обладателями которой являются ГБУ ВО РИАЦОКО или его контрагенты;

– создает работнику необходимые условия для соблюдения им установленного ГБУ ВО РИАЦОКО режима конфиденциальной информации;

– обеспечивает заключение с контрагентами ГБУ ВО РИАЦОКО, в том числе с лицами, выполняющими работы (оказывающими услуги) в пользу ГБУ ВО РИАЦОКО на основании гражданско-правовых договоров, соглашений о неразглашении КИ;

– исполняет иные обязанности, предусмотренные Положением.

8.2.3. Если информация, в отношении которой целесообразно установление режима КИ, получена в ходе выполнения работ по договору или реализации соглашения, в целях определения конкретных сведений, подлежащих защите, необходимых мер по защите информации, а также для урегулирования иных вопросов, заведующий отделом, ответственный за исполнение договора (соглашения) со стороны ГБУ ВО РИАЦОКО, вносит предложения по включению в соответствующий договор (соглашение) положений, определяющих взаимные обязательства и ответственность сторон за ее сохранность.

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

8.3 Ответственность за нарушение режима конфиденциальности основывается на принципе персональной ответственности, который заключается в том, что каждое лицо, разрешающее доступ и/или получившее доступ к КИ, должно лично отвечать за свою деятельность, включая любые действия с КИ 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 КИ.

8.4 Лица, разгласившие конфиденциальную информацию, и/или иным образом нарушившие установленную Положением разрешительную систему доступа, работы и хранения КИ, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

8.5 Нарушением режима КИ признаются, в том числе:

- разглашение КИ;
- неправомерное использование КИ;
- несанкционированный доступ к КИ;
- утрата документов и иных материальных носителей, содержащих КИ;
- неправомерное уничтожение документов, содержащих КИ;

– нарушение требований хранения документов, содержащих КИ;
– другие нарушения требований законодательства и настоящего Положения.

9. Защита конфиденциальной информации. Технические каналы утечки защищаемой КИ, циркулирующей на объектах информатизации.

9.1. Технический канал утечки информации (ТКУИ) представляет собой совокупность следующих факторов:

- источника информативного сигнала;
- физической среды его распространения;
- приемника, способного зарегистрировать данный сигнал.

9.2. При ведении переговоров и использовании технических средств для обработки и передачи информации на объектах информатизации организации возможна реализация следующих ТКУИ:

- акустического излучения информативного речевого сигнала;
- электрических сигналов, возникающих при преобразовании информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющихся по проводам и линиям, выходящим за пределы КЗ;
- НСД к обрабатываемой в АС информации и несанкционированные действия с ней;
- воздействия на технические или программные средства АС в целях нарушения конфиденциальности, целостности и доступности информации посредством специально внедренных программных средств;
- ПЭМИН информативных сигналов от технических средств АС и линий передачи информации;
- наводок информативного сигнала, обрабатываемого техническими средствами АС, на цепи электропитания и линии связи, выходящие за пределы КЗ;
- радиоизлучений, модулированных информативным сигналом, возникающим при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучений или электрических сигналов от внедренных в технические средства и защищаемые помещения специальных электронных устройств съема речевой информации ("закладочные устройства"), модулированных информативным сигналом;
- радиоизлучений или электрических сигналов от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- просмотра информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств;
- прослушивания телефонных и радиопереговоров;
- хищения технических средств с хранящейся в них информацией или носителей информации.

9.3. Перехват информации, циркулирующей на объекте информатизации, или воздействие на нее с использованием технических средств могут вестись:

- из смежных помещений, принадлежащих другим организациям и расположенным в том же здании, что и объект информатизации;
- при посещении организации посторонними лицами;
- за счет НСД к информации, циркулирующей в информационной системе, как с помощью технических средств автоматизированной системы, так и через сети.

Защита информации, циркулирующей на объекте информатизации, должна быть комплексной и дифференцированной. С этой целью для каждого объекта информатизации создается система защиты информации.

9.4. Комплексная защита информации на объектах информатизации проводится по

следующим основным направлениям работы:

- охрана помещений объекта;
- определение перечня информации, подлежащей защите;
- классификация информационных систем;
- создание системы защиты информации при разработке и модернизации объекта;
- составление организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;
- защита речевой информации при осуществлении конфиденциальных переговоров;
- защита информации, содержащей КИ, при обработке, передаче с использованием технических средств, а также на бумажных или иных носителях;
- защита информации при взаимодействии абонентов с информационными сетями связи общего пользования.

9.5. Перечень необходимых мер защиты информации определяется по результатам обследования объекта информатизации с учетом соотношения затрат на защиту информации с возможным ущербом от ее разглашения, утраты, уничтожения, искажения, нарушения санкционированной доступности и работоспособности технических средств, обрабатывающих эту информацию, а также с учетом реальных возможностей ее перехвата и раскрываемости.

9.6. Основное внимание должно быть уделено защите информации, содержащей КИ, в отношении которой угрозы реальны и сравнительно просто реализуемы без применения сложных технических средств перехвата информации. К информации такого рода относится:

- речевая информация, циркулирующая в защищаемом помещении;
- информация, обрабатываемая СВТ;
- информация, выводимая на экраны мониторов;
- документированная информация, содержащая КИ;
- информация, передаваемая по каналам связи, выходящим за пределы КЗ.

10. Порядок уничтожения конфиденциальной информации

10.2. КИ, утратившая практическую значимость данных, а также с вышедшими сроками хранения, утилизируется.

10.3. Процесс уничтожения КИ происходит в следующей последовательности:

10.3.2. Экспертиза ценности КИ;

10.3.3. Выделение конфиденциальных материалов к уничтожению (документов, любых носителей информации);

10.3.4. Составление описи ликвидируемой КИ;

10.3.5. Согласование утилизации КИ с лицом, ответственным за обеспечение требований по защите информации (письменное разрешение);

10.3.6. Оформление акта на уничтожение;

10.3.7. Ликвидация документов по акту.

10.4. Составление акта утилизации обязательно для дел, документов, видео- и аудиоматериалов, проекты документов, картотек, черновиков, описей, а также электронных документов или ссылки на них, которые хранятся в памяти компьютера либо на магнитных носителях.

10.5. В случае уничтожения конфиденциальной документации в не ГБУ ВО РИАЦОКО необходимо обеспечить ее безопасную доставку на утилизацию, исключающую возможность доступа посторонних. КИ помещается в опломбированные короба, перевозятся на служебном автомобиле, под сопровождением персонала учреждения.

Приложение № 1
к Положению КИ
в ГБУ ВО РИАЦОКО

Форма

СОГЛАШЕНИЯ
о неразглашении конфиденциальной информации

г. Владимир «___» _____20___г.

Государственное бюджетное учреждение Владимирской области «Региональный информационно – аналитический центр оценки качества образования» (далее – ГБУ ВО РИАЦОКО в лице **директора Мансуровой Светланы Ивановны**, действующего на основании **Устава**, с одной стороны и **гражданина Российской Федерации**, в лице [**должность, Ф. И. О.**],получающий доступ к конфиденциальной информации, действующего на основании [**паспортные данные, реквизиты документа о приеме на работу**], с другой стороны, совместно именуемые «Стороны», заключили настоящее соглашение о нижеследующем:

1. В соответствии с условиями настоящего соглашения устанавливаются обязательные для Сторон требования по защите Информации, переданной одной стороной другой стороне.

1.1. Под **Информацией** в настоящем соглашении понимается информация, определенная настоящим соглашением как конфиденциальная.

1.2. Под **защитой Информации** в настоящем соглашении понимается обязанность Сторон поддерживать полную конфиденциальность полученной друг от друга информации, не раскрывать ее содержание и источники получения третьим лицам, а также не использовать указанную информацию во вред второй стороне.

2.Стороны устанавливают режим конфиденциальности в отношении следующей информации, не составляющей государственную, коммерческую или иную охраняемую законом тайну (отметить нужное):

Отметка (V - да, х – нет)	**Сведения, отнесенные к категории** **ограниченного доступа**	**Основания отнесения сведений к категории ограниченного доступа**
	Персональные данные (любая информация, относящаяся прямо или косвенно к определенному или определяемому лицу).	Статья 7 Федерального закона от 27.06.2006 года №152-ФЗ «О персональных данных».
	Сведения, ставшие известными в связи с исполнением должностных обязанностей, в том числе сведения, касающиеся частной жизни и здоровья граждан или затрагивающие их честь и достоинство.	Пункт 6 статьи 12 Федерального закона от 02.03.2007 года №25-ФЗ «О муниципальной службе в Российской Федерации».
	Сведения о личной и семейной тайне. Сведения, раскрывающие тайну переписки, телефонных переговоров, почтовых и иных сообщений.	Статья 23 Конституции Российской Федерации, принятой всенародным голосованием 12 декабря 1993 года.
	Сведения, содержащиеся в проектах документов (или) прилагаемых к ним материалах на любом носителе информации, до официальной публикации.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».
	Сведения, содержащиеся в материалах служебных расследований (проверок), до издания соответствующих распорядительных документов.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о

		защите информации».
	Сведения о системах защиты информации (средства, методы и способы защиты информации, реквизиты доступа, модели угроз, технические паспорта информационных систем, матрицы доступа, пароли, ключи электронной подписи, процедуры доступа к информационным системам и ресурсам). Сведения об оценке эффективности защиты информации.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации». Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
	Сведения об информационно-телекоммуникационных сетях и каналах связи, компьютерных сетях, системах и средствах охранно-тревожной, пожарной сигнализации и видеонаблюдения.	Пункт 3 статьи 6 Федерального закона от 27.07.2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации».

4. В рамках настоящего соглашения **конфиденциальной не считается информация**, которая:
- является общеизвестной или общедоступной;
- стала известна одной из сторон от третьего лица, а не от первой стороны настоящего соглашения;
- была известна стороне до подписания настоящего соглашения;
- была самостоятельно разработана разглашающей стороной;
- разрешена к ее раскрытию первой стороной настоящего соглашения;
- [**указать иное:**_____].

5. В целях исполнения условий настоящего соглашения Стороны принимают на себя следующие **обязательства**:

5.1. Получать, хранить и защищать Информацию от ее несанкционированного использования или раскрытия.

5.2. Без разрешения первой стороны не публиковать, не раскрывать и не передавать Информацию третьим лицам.

5.3. Осуществлять передачу Информации только следующими способами, утвержденными нормативными локальными актами ГБУ ВО РИАЦОКО.

5.4. Стороны обязуются не передавать друг другу Информацию по открытым каналам телефонной, телеграфной и факсимильной связи, а также с использованием сети Интернет.

5.5. Не использовать полученную Информацию в целях незаконной конкуренции, а также в любой деятельности, способной причинить вред первой стороне.

5.6. Довести до сведения всех лиц, имеющих доступ к указанной Информации, положения настоящего соглашения.

5.7. Не допускать доступа к Информации лиц, которые работают или работали на одну из сторон настоящего соглашения по найму, если этой стороне не удастся сохранить конфиденциальность Информации в будущем.

5.8. Передавать второй стороне по **акту приема-передачи** Информацию в объеме согласно п. 2 настоящего соглашения.

5.9. Соблюдать такую же высокую степень секретности во избежание разглашения или использования этой Информации, какую каждая из сторон соблюдала бы в разумной степени в отношении своей собственной конфиденциальной Информации такой же степени важности.

5.10. Уничтожить или передать раскрывающей стороне в соответствии с указаниями после использования все материальные носители, а также снятые с них копии, технические и программные средства, содержащие конфиденциальную Информацию.

6. Стороны несут ответственность за умышленное или неосторожное разглашение Информации третьим лицам.

7. В случае нарушения условий настоящего соглашения вторая сторона, причинившая первой стороне убытки, обязана их возместить в полном объеме.

8. Споры и разногласия, которые могут возникнуть при исполнении настоящего соглашения, будут по возможности разрешаться путем переговоров между Сторонами.

В случае, если Стороны не придут к соглашению, споры разрешаются в соответствии с действующим законодательством РФ во Владимирском Арбитражном суде.

9. Передача Информации третьим лицам допускается только с предварительного

письменного разрешения первой стороны.

9.1. Передача Информации без письменного согласия первой стороны допускается только в случаях, предусмотренных действующим законодательством РФ.

10. В соответствии с условиями настоящего соглашения после передачи Информация остается собственностью передающей Стороны.

11. Во всем остальном, что не предусмотрено настоящим соглашением, Стороны руководствуются действующим законодательством РФ.

12. Все изменения и дополнения к настоящему соглашению оформляются в письменном виде.

13. Настоящее соглашение вступает в законную силу с момента его подписания Сторонами и действует до [**число, месяц, год**].

14. Соглашение составлено в 2-х (двух) подлинных экземплярах, по одному экземпляру для каждой Стороны и оба экземпляра имеют одинаковую юридическую силу.

15. Неотъемлемой частью настоящего соглашения является:

- Приложение - Акт приема-передачи информации.

16. Реквизиты и подписи сторон:

[**Наименование юридического лица**] [**вписать нужное**] [**должность, подпись, инициалы, фамилия**] М. П.	[**Наименование юридического лица**] [**вписать нужное**] [**должность, подпись, инициалы, фамилия**] М. П.

Приложение
к соглашению о неразглашении
конфиденциальной информации

Акт приема-передачи информации

г. Владимир **[число, месяц, год]**

[Полное наименование юридического лица], в лице [**должность, Ф. И. О.**], действующего на основании [**наименование документа, подтверждающего полномочия**], с одной стороны и

[полное наименование юридического лица], в лице [**должность, Ф. И. О.**], действующего на основании [**наименование документа, подтверждающего полномочия**], с другой стороны, и вместе именуемые "Стороны", подписали настоящий акт о нижеследующем:

1. В соответствии с условиями соглашения о конфиденциальности N [**значение**] от [**число, месяц, год**] [**наименование юридического лица**] передает, а [**наименование юридического лица**] принимает следующую конфиденциальную информацию:

N п/п	Наименование документа	Кол-во листов	Тип носителя	Примечание
1	2	3	4	5

2. В свою очередь [**наименование юридического лица**] передает, а [**наименование юридического лица**] принимает следующую конфиденциальную информацию:

N п/п	Наименование документа	Кол-во листов	Тип носителя	Примечание
1	2	3	4	5

3. С момента подписания настоящего акта в отношении переданной информации Сторонами устанавливается режим защиты информации: [**вписать нужное**].

4. Настоящий акт составлен в двух экземплярах, по одному для каждой из Сторон.

[Наименование юридического лица]
[вписать нужное]
[должность, подпись, инициалы, фамилия]
М. П.

[Наименование юридического лица]
[вписать нужное]
[должность, подпись, инициалы, фамилия]
М. П.