

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное
образовательное учреждение высшего образования
«Череповецкий государственный университет»

УТВЕРЖДЕНО
приказом ректора
№ 05-02-106 от 30.11.2023

Система менеджмента качества
ПОЛОЖЕНИЕ О ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
ЧЕРЕПОВЕЦКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

наименование документа

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение о защите конфиденциальной информации Череповецкого государственного университета (далее – Положение) определяет порядок использования работниками федерального государственного бюджетного образовательного учреждения высшего образования «Череповецкий государственный университет» (далее – Череповецкий государственный университет, Университет) и иными лицами, вовлеченными в научно-образовательные проекты, реализуемые в Университете, информации, отнесенной к конфиденциальной; порядок обеспечения защиты конфиденциальной информации; полномочия и обязанности работников и иных лиц в части обеспечения конфиденциальности информации.

1.2. Действие настоящего Положения распространяется на всех работников Университета, а также иных лиц, подписавших обязательство о неразглашении конфиденциальной информации.

1.3. Положение разработано в соответствии с требованиями следующих нормативно-правовых актов:

- Конституция Российской Федерации,
- Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных» (с изменениями и дополнениями);
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями);
- Федеральный закон от 29 июля 2004 г. N 98-ФЗ «О коммерческой тайне» (с изменениями и дополнениями);
- Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями и дополнениями);
- устав Университета;
- иные локальные нормативные акты Университета в сфере защиты конфиденциальной информации и коммерческой тайны.

1.4. Составной частью информации, в отношении которой действует режим конфиденциальности, являются секреты производства (ноу-хау), отнесенные к коммерческой тайне Университета. Порядок отнесения информации к секретам производства (ноу-хау), а также режим коммерческой тайны и способы его защиты определяются Положением о секретах производства (ноу-хау) Череповецкого государственного университета, составляющих коммерческую тайну.

1.5. Действие Положения направлено на введение в Университете разрешительной системы доступа к конфиденциальной информации допускаемых лиц (далее – разрешительная система доступа).

2. ОСНОВНЫЕ ПОНЯТИЯ И ТЕРМИНЫ

В Положении используются следующие понятия:

2.1. **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 Череповецкого государственного университета, его работников и обучающихся, и в отношении которой Университетом введен режим конфиденциальности информации.

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

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

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

2.3. **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;

2.4. **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;

2.5. **конфиденциальность информации** – требование не разглашать информацию третьим лицам без согласия ее обладателя, обязательное для выполнения лицом, получившим доступ к определенной 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. **обладатель информации** – юридическое лицо (ЧГУ 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;

2.9. **допуск к конфиденциальной информации** – выполнение обладателем информации (уполномоченным должностным лицами Университета) 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;

2.10. **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);

2.11. **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.

2.12. **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. **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;

2.14. **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;

2.15. **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;

2.16. **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

2.17. **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;

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

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

2.20. **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;

2.21. **работник Череповецкого государственного университета** – физическое лицо, вступившее в трудовые отношения с Университетом;

2.22. **куратор договора** – работник Университета, назначенный руководителем структурного подразделения (управления, отдела) для организации заключения договора (контракта), сопровождения исполнения договора (контракта), в т.ч. приемки и проверки качества (экспертизы) товара, работ, услуг, отвечающий за подготовку и согласование договора по соответствующему направлению деятельности;

2.23. **обучающийся** – физическое лицо, осваивающее образовательную программу в Университете.

3. ПОРЯДОК ОТНЕСЕНИЯ ИНФОРМАЦИИ К КАТЕГОРИИ КОНФИДЕНЦИАЛЬНОЙ

3.1. Конфиденциальной информацией Череповецкого государственного университета признаются следующие сведения:

3.1.1. Персональные данные работников и обучающихся, обрабатываемые Череповецким государственным университетом;

3.1.2. Информация, составляющая коммерческую тайну, к которой Университетом отнесены секреты производства (ноу-хау). Режим коммерческой тайны в отношении секретов производства (ноу-хау) и способы их защиты, формы оформляемых документов определяются Положением о секретах производства (ноу-хау) Череповецкого государственного университета, составляющих коммерческую тайну.

3.1.3. Иные сведения конфиденциального характера, признанные Университетом как подлежащие защите, и разглашение которых может нанести материальный, репутационный или иной ущерб Череповецкому государственному университету. Перечень иных сведений конфиденциального характера приведен в Приложении 1 к настоящему Положению.

3.2. К сведениям конфиденциального характера, в том числе, к коммерческой тайне, не могут быть отнесены следующие сведения:

3.2.1. содержащиеся в учредительных документах Университета, документах, подтверждающих факт внесения записей о юридическом лице и об индивидуальных предпринимателях в соответствующие государственные реестры;

3.2.2. содержащиеся в документах, дающих право на осуществление предпринимательской деятельности контрагентам Университета;

3.2.3. о 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 Университета 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 Университета, о размерах и составе его имущества, о его расходах, о численности и об оплате труда работников, об использовании безвозмездного труда граждан в деятельности Университета;

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.

3.2.10. составляющих информацию о состоянии окружающей среды (экологическую информацию).

3.3. Отношения Университета и физических лиц, возникающие в связи с обработкой их персональных данных, регулируются Положением о работе с персональными данными в Череповецком государственном университете.

3.4. Руководители структурных подразделений Университета, в деятельности которых присутствуют процессы обработки конфиденциальной информации, имеют право инициировать актуализацию перечня иных сведений конфиденциального характера.

3.5. 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 Череповецкого государственного университета.

3.6. Режим конфиденциальности информации Университета действует:

3.6.1. для персональных данных, обрабатываемых Череповецким государственным университетом – до прекращения деятельности Университета;

3.6.2. для информации, отнесенной к конфиденциальной в соответствии с настоящим Положением – в течение срока действия обязательств о неразглашении конфиденциальной информации.

3.6.3. для секретов производства (ноу-хау), составляющих коммерческую тайну, - в течение срока, определяемого Положением о секретах производства (ноу-хау) Череповецкого государственного университета, составляющих коммерческую тайну;

3.6.4. для конфиденциальной информации, полученной от контрагентов Университета, – в течении 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:

4.2.4. размещенной в информационных системах в форме электронного документа;

4.2.5. 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 ЧГУ 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 к конфиденциальной информации:

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 К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

6.1. К лицам, имеющим доступ к конфиденциальной информации без прохождения процедуры допуска в силу должностных обязанностей и ответственным за организацию разрешительной системы доступа к конфиденциальной информации в Университете относятся:

6.1.1. ректор;

6.1.2. первый проректор, проректоры, главный бухгалтер;

6.2. К лицам, которым оформляется допуск к конфиденциальной информации при заключении трудового договора и обеспечивается доступ к данной информации при исполнении трудовых обязанностей, относятся:

6.2.1. директора институтов, декан факультета, заведующие кафедрами;

6.2.2. руководители структурных подразделений Университета – управлений, отделов.

6.3. Под допускаемыми к конфиденциальной информации лицами в Университете

понимаются:

- 6.3.1. работники Университета;
- 6.3.2. лица, выполняющие работу или оказывающие услуги на основании гражданско-правовых договоров с Университетом;
- 6.3.3. лица, обучающиеся в Университете по образовательным программам;
- 6.3.4. иные лица (в том числе контрагенты или 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 (при заключении с допускаемыми лицами договоров гражданско-правового характера);

7.1.3. конфиденциальная информация 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 обеспечивается допуск к конфиденциальной информации при исполнении трудовых обязанностей (п. 6.2. Положения), а также работники, которым для выполнения своих трудовых обязанностей необходимо иметь доступ к конфиденциальной информации, перечисленной в п. 3.1. Положения, как при приеме на работу, так и в период работы в Череповецком государственном университете, должны быть ознакомлены с настоящим Положением, перечнем конфиденциальной информации Череповецкого государственного университета, предупреждены об ответственности за разглашение сведений, содержащих конфиденциальную информацию. Указанные работники должны дать письменное обязательство о неразглашении указанных сведений в соответствии с формой СМК Ф 5.5.0-01-01.

Работники имеющие доступ к конфиденциальной информации без прохождения процедуры допуска в силу должностных обязанностей (п. 6.1. Положения), несут ответственность за нарушение процедуры работы с информацией, отнесенной к конфиденциальной, в соответствии с настоящим Положением.

7.3. Исполнители (подрядчики) – физические лица, которым для оказания услуг (выполнения работ) необходимо иметь доступ к конфиденциальной информации, перечисленной в п. 3.1. Положения, должны быть ознакомлены с настоящим Положением, перечнем конфиденциальной информации Череповецкого государственного университета, предупреждены об ответственности за разглашение сведений, содержащих конфиденциальную информацию, и должны подписать соглашение о неразглашении конфиденциальной информации в соответствии с формой СМК Ф 5.5.0-01-02.

7.4. Исполнители (подрядчики) – юридические лица, которым для оказания услуг (выполнения работ) необходимо иметь доступ к конфиденциальной информации, перечисленной в п. 3.1. Положения, должны подписать соглашение о неразглашении конфиденциальной информации в соответствии с формой СМК Ф 5.5.0-01-03.

7.5. Предусмотренные пп. 7.2, 7.3., 7.4. формы могут изменяться либо корректироваться по инициативе руководителя структурного подразделения или куратора

соответствующего договора по согласованию с административно-правовым управлением Университета.

7.6. Руководители управлений, отделов, директора институтов, декан факультета, заведующие кафедрами обязаны разъяснять допускаемым лицам из числа работников (в том числе поступающим на работу) особенности порядка обращения с конфиденциальной информацией, в том числе с персональными данными. Инструктаж проводится в объеме настоящего Положения и других локальных нормативных актов, регламентирующих обеспечение сохранности конфиденциальной информации, в том числе персональных данных.

7.7. Допускаемые к сведениям конфиденциального характера работники Университета, исполнители (подрядчики) по договорам получают доступ к конфиденциальной информации в объеме, необходимом для выполнения ими своих трудовых обязанностей, обязанностей по договору с разрешения руководителя структурного подразделения (куратора договора) и на основании прохождения процедуры допуска к конкретной конфиденциальной информации путем подписания обязательств, соглашений.

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

7.9. Руководители управлений, отделов, директора института, декан факультета, заведующие кафедрами, кураторы договоров осуществляют фиксацию допуска работника своего структурного подразделения, исполнителя (подрядчика) по договору к сведениям, отнесенным к конфиденциальной информации (в том числе к персональным данным). Соответствующая запись производится в Журнале учета лиц, получивших допуск к конфиденциальной информации (СМК Ф 5.5.0-01-04). Журнал учета должен быть распечатан, прошит, пронумерован; храниться у соответствующего руководителя подразделения, куратора договора в течение 3-х лет после совершения в нем последней записи. При смене руководителя новому руководителю должен быть передан прежний журнал, и ведение журнала на следующий период осуществляется заново.

7.10. После оформления допуска работников Университета, исполнителей (подрядчиков) по договорам и их работников к сведениям конфиденциального характера, разрешается доступ указанных лиц к сведениям конфиденциального характера Университета. Ответственность за несанкционированное разглашение конфиденциальной информации лицами, допущенными к сведениям конфиденциального характера без соответствующего оформления допуска к ним, несут работники Университета, перечисленные в пп. 6.1.3, 6.1.4., ответственные работники управления персонала, кураторы договоров.

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 после письменного согласования с руководителем структурного подразделения (проставление визы на запросе (письме) или в письменного согласования в корпоративной электронной почте).

8.3. 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 Университета, обязаны:

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

9.1.2. при работе с конфиденциальной информацией, в том числе с коммерческой тайной, 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 корпоративных информационных систем и сервисов, 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 недостатке документов, содержащих конфиденциальную информацию, ключей от сейфов (хранилища), печатей, удостоверений, пропусков, а также о любых иных обстоятельствах, создающих угрозу конфиденциальности информации Университета;

9.1.5. при возникновении необходимости в передаче конфиденциальной информации по электронной почте третьим лицам не осуществлять передачу конфиденциальной информации с использованием иных средств, чем корпоративная электронная почта Университета (если иное не предусмотрено в отдельном соглашении или обязательстве о неразглашении);

9.1.6. при передаче конфиденциальной информации в электронной форме по корпоративной электронной почте Университета как работникам Университета, так и третьим лицам включить в исходящее письмо и в последующую переписку уведомление о конфиденциальности в следующей форме: «Это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию и предназначены исключительно для использования работниками Череповецкого государственного 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.»;

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) любых лиц, кроме лиц, допущенных к конфиденциальной информации в установленном порядке;

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 и согласования представителя службы комплексной безопасности 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 информации¹;

9.2.7. самовольно подключать периферийные устройства² 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 управлением информационных технологий Череповецкого государственного университета.

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

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 Череповецкого государственного 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 Череповецкого государственного 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), начальнику службы комплексной безопасности, начальнику управления информационных технологий.

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

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).

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 (управления, отдела), директор института, декан факультета, заведующий кафедрой:

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 настоящим 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 заключение с контрагентами Университета, в том числе с лицами, выполняющими работы (оказывающими услуги) в пользу Университета на основании гражданско-правовых договоров, соглашений 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.

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. Нарушением режима конфиденциальности информации признаются, в том числе:

10.2.1. разглашение конфиденциальной информации;

10.2.2. неправомерное использование конфиденциальной информации;

10.2.3. несанкционированный доступ к конфиденциальной информации;

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

10.2.5. неправомерное уничтожение документов, содержащих конфиденциальную информацию;

10.2.6. нарушение требований хранения документов, содержащих конфиденциальную информацию;

10.2.7. другие нарушения требований законодательства и настоящего Положения.

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

10.3.1. Административная ответственность: разглашение информации с ограниченным доступом (статья 13.14. КоАП РФ).

10.3.2. Уголовная ответственность: незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (статья 183 УК РФ); нарушение неприкосновенности частной жизни (ст. 137 УК РФ).

10.3.3. Гражданско-правовая ответственность за разглашение коммерческой тайны может выражаться в возмещении убытков и(или) в обязанности заплатить неустойку, если она была предусмотрена договором в качестве санкции за данное нарушение (ст.ст. 15, 330, 393 ГК РФ), а также в ответственности за нарушение исключительного права на секрета производства (ст.1472 ГК РФ).

Гражданско-правовая ответственность за нарушение прав субъекта персональных данных установлена ст.ст. 15,151,1099-1101 ГК РФ, ст. 24 ФЗ «О персональных данных».

10.3.4. За разглашение персональных данных работники Университета могут быть привлечены к дисциплинарной ответственности в виде замечания, выговора, увольнения (пп. «в» п.6 ч.1 ст. 81, ст. 192 ТК РФ).

За ущерб, причиненный работодателю, в том числе, если по вине работника работодатель должен возместить ущерб, причиненный работником третьему лицу, работник несет материальную ответственность (ст. 239 ТК РФ)

11. ЗАКЛЮЧИТЕЛЬНЫЕ И ПЕРЕХОДНЫЕ ПОЛОЖЕНИЯ

11.1. Утверждение настоящего Положения, внесение изменений в настоящее Положение, а также утверждение Положения в новой редакции осуществляется на основании приказа ректора Университета или иного уполномоченного лица.

11.2. Настоящее Положение вступает в силу со дня утверждения его приказом ректора Университета.

11.3. Директора институтов, декан факультета, заведующие кафедрами, руководители структурных подразделений (управлений, отделов), должны обеспечивать своевременное оформление доступа к конфиденциальной информации Университета (при необходимости) работникам координируемых структурных подразделений и иным лицам, перечисленным в п. 6.3. Положения, путем уведомления по корпоративной электронной почте управления персонала или кураторов заключаемых договоров о необходимости подписания работниками обязательств о неразглашении конфиденциальной информации, заключения с исполнителями (подрядчиками) соглашений о неразглашении конфиденциальной информации по установленным формам.

11.4. Директора институтов, декан факультета, заведующие кафедрами, руководители структурных подразделений (управлений, отделов) обязаны подписать обязательства о неразглашении конфиденциальной информации по установленной форме не позднее 14 календарных дней с даты вступления в силу настоящего Положения.

11.5. Директора институтов, декан факультета, заведующие кафедрами, руководители структурных подразделений (управлений, отделов) обязаны в срок не позднее 30 рабочих дней со дня вступления в силу настоящего Положения направить информацию (уведомления, списки) в управление персонала и кураторам договоров в отношении действующих

работников Университета и исполнителей (подрядчиков) по договорам гражданско-правового характера о необходимости подписания обязательств, соглашений.

11.6. Директора институтов, декан факультета, заведующие кафедрами, руководители структурных подразделений (управлений, отделов) обязаны не позднее даты заключения трудового или гражданско-правового договора с лицами, которым требуется допуск к сведениям конфиденциального характера направлять информацию (уведомления) в управление персонала и кураторам договоров в отношении принимаемых на работу лиц и исполнителей (подрядчиков) по договорам гражданско-правового характера о необходимости подписания обязательств, соглашений;

11.7. Ответственные работники управления персонала и кураторы договоров обязаны не позднее 3-х рабочих дней после получения уведомлений, полученных в порядке п. 11.5, 11.6. Положения, но не позднее даты подписания трудового, гражданско-правового договора, обеспечить подписание работниками Университета, исполнителями (подрядчиками) по договорам обязательств (соглашений) о неразглашении сведений конфиденциального характера.

12. ФОРМЫ ДОКУМЕНТОВ (ЗАПИСЕЙ) ПО ПРОЦЕССУ

СМК Ф 5.5.0-01-01	Форма обязательства о неразглашении конфиденциальной информации
СМК Ф 5.5.0-01-02	Форма соглашения о неразглашении конфиденциальной информации (для физических лиц)
СМК Ф 5.5.0-01-03	Форма соглашения о неразглашении конфиденциальной информации (для юридических лиц)
СМК Ф 5.5.0-01-04	Журнал учета лиц, получивших допуск к конфиденциальной информации университета

**ПЕРЕЧЕНЬ ИНЫХ СВЕДЕНИЙ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА
ЧЕРЕПОВЕЦКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА**

№	Направления деятельности	Лица, уполномоченные на предоставление допуска и доступа к конфиденциальной информации работникам структурных подразделений, исполнителям (подрядчикам) по договорам	Перечень конфиденциальной информации, к которой предоставляется доступ работникам Университета соответствующего структурного подразделения в соответствии с обязательством о неразглашении
1	По всем направлениям деятельности	Руководители всех структурных подразделений Университета	<ol style="list-style-type: none">1. Информация о хозяйственно-финансовых отношениях с деловыми партнерами (в том числе условия договорных отношений с ними), о проведении переговоров, переписке с ними.2. Информация, составляющая электронную базу Университета (списки, перечни, информационные системы), содержащая сведения об обучающихся, работниках, деловых партнерах Университета;3. Условия заключаемых сделок, за исключением сделок, которые размещаются в ЕИС или подлежат обязательному доведению до сведения любых заинтересованных лиц;4. Содержание работ, проводимых на основании договоров с контрагентами;5. Сведения о контрагентах Университета которые не содержатся в открытых источниках (справочниках, каталогах и др.): состояние расчетов с контрагентами, включая активы контрагентов; состав поручений контрагентов; адреса, телефоны, сведения об имущественных правах, аффилированных лицах, деловых связях, финансовом и экономическом состоянии и т.п.) а также персональная информация о работниках контрагентов;6. Сведения о подготовке, принятии и исполнении решений руководства Университета по вопросам его деятельности, развития, а также по иным организационным, финансовым и научно-техническим вопросам;

№	Направления деятельности	Лица, уполномоченные на предоставление допуска и доступа к конфиденциальной информации работникам структурных подразделений, исполнителям (подрядчикам) по договорам	Перечень конфиденциальной информации, к которой предоставляется доступ работникам Университета соответствующего структурного подразделения в соответствии с обязательством о неразглашении
			<p>7. Идентификаторы и пароли, используемые работниками Университета для доступа в служебные помещения, к информации и ресурсам Университета в электронном виде;</p> <p>8. 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;</p> <p>9. Информация о личных отношениях работников как между собой, так и с руководством, сведения о возможных противоречиях, конфликтах внутри коллектива (за исключением сведений о конфликте интересов, способным повлиять на исполнение должностных обязанностей);</p> <p>10. Сведения о необъявленных официально планах Университета вывода на рынок новых результатов НИР, а также образовательных услуг и программ;</p> <p>11. Сведения о результатах интеллектуальной деятельности, исключительное право на которые принадлежит Университету, до получения ими правовой охраны / защиты;</p> <p>12. Отчетные документы по результатам внутренних (служебных) проверок;</p> <p>13. Тексты проектов приказов и распоряжений, которые готовятся руководителями структурных подразделений в соответствии с локальными нормативными актами Университета.</p> <p>14. Проекты локальных нормативных актов Университета, утвержденные локальные нормативные акты, необходимые работнику в связи с выполнением должностных обязанностей</p>

№	Направления деятельности	Лица, уполномоченные на предоставление допуска и доступа к конфиденциальной информации работникам структурных подразделений, исполнителям (подрядчикам) по договорам	Перечень конфиденциальной информации, к которой предоставляется доступ работникам Университета соответствующего структурного подразделения в соответствии с обязательством о неразглашении
			<p>15. Переписка с Минобрнауки России и иными государственными органами, органами местного самоуправления, контрагентами в пределах вопросов структурного подразделения.</p> <p>16. Содержание переписки, документов, доступные работнику в корпоративной электронной почте Университета, на иных ресурсах, используемых в Университете.</p>
2	Деятельность по общему делопроизводству	Начальник отдела делопроизводства административно-правового управления	1. Входящая (за исключением входящих рекламных предложений) и исходящая корреспонденция (в том числе в электронном виде)
3	Деятельность по ведению архива Череповецкого государственного университета	Начальник административно-правового управления	<p>1. Архивные документы кадрового делопроизводства;</p> <p>2. Архивные документы по обучающимся</p> <p>3. Архивные научно-технические документы (отчеты по НИР)</p>
4	Внутренняя деятельность военного учебного центра	Начальник военного учебного центра	<p>1. Переписка с органами военного управления по вопросам наличия и содержания образцов вооружения и военной техники, комплектования ВУЦ данными образцами в соответствии с табелем вооружения.</p> <p>2. Сведения, содержащиеся в нормативно-правовых актах МО РФ с грифом дсп.</p> <p>3. Материалы расследований и разбирательств.</p> <p>4. Документы по планированию, организации образовательной деятельности в ВУЦ.</p> <p>5. Документы учета обучающихся и их персонального учета, личные карточки обучающихся.</p>

№	Направления деятельности	Лица, уполномоченные на предоставление допуска и доступа к конфиденциальной информации работникам структурных подразделений, исполнителям (подрядчикам) по договорам	Перечень конфиденциальной информации, к которой предоставляется доступ работникам Университета соответствующего структурного подразделения в соответствии с обязательством о неразглашении
			5. Донесения об укомплектованности должностными лицами и основных показателях деятельности военного учебного центра. 7. Доклады об итогах военной подготовки граждан и проведении учебных сборов (отчеты о выполнении программ учебных сборов). 8. Документы конкурсного отбора граждан, изъявивших желание пройти военную подготовку. 9. Документы учета и обслуживания вооружения, военной техники и военно-учебного имущества. 10. Документы кадрового учета, личные дела военнослужащих и обучающихся. 11. Результаты контроля организации деятельности ВУЦ комиссиями МО РФ.
5	Деятельность по обеспечению безопасности	Начальник службы комплексной безопасности	1. Сведения о порядке и состоянии организации безопасности и системе охраны, пропускном режиме, противопожарной безопасности, систем сигнализации. 2. Переписка с контролирующими и правоохранительными органами. 3. Материалы внутренних расследований и разбирательств, служебных проверок.
6	Закупочная деятельность	Начальник управления закупок, договорной деятельности и имущественных отношений	1. Сведения о готовящихся торгах и документация о таких торгах до их объявления.
7	Деятельность по связям с общественностью	Начальник управления коммуникацией и PR-сопровождения	1. Сведения о планах Университета в отношении формирования публичной информационной политики: детали внутренних графиков встреч, мероприятий, в отношении которых руководство Университета приняло решение не информировать общественность.

№	Направления деятельности	Лица, уполномоченные на предоставление допуска и доступа к конфиденциальной информации работникам структурных подразделений, исполнителям (подрядчикам) по договорам	Перечень конфиденциальной информации, к которой предоставляется доступ работникам Университета соответствующего структурного подразделения в соответствии с обязательством о неразглашении
8	Деятельность по подбору персонала и кадровая работа	Начальник управления персонала	1. Сведения о размере заработной платы работников Университета; сведения о принятии решений, касающихся материального стимулирования работников, в том числе о процедуре согласования материального стимулирования; 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. 4. Информация о нарушениях работниками трудового законодательства и локальных нормативных актов Университета
9	Финансовая, и бухгалтерская деятельность	Главный бухгалтер - начальник управления учета, отчетности и финансового контроля и его заместители	1. Сведения о размере заработной платы работников Университета; о принятии решений, касающихся материального стимулирования работников, в том числе о процедуре согласования материального стимулирования. 2. 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: <ul style="list-style-type: none"> - образцы подписей физических лиц; - документы, содержащие сведения о получаемых и предлагаемых предложениях; - деловая переписка; - протоколы закрытых совещаний;

№	Направления деятельности	Лица, уполномоченные на предоставление допуска и доступа к конфиденциальной информации работникам структурных подразделений, исполнителям (подрядчикам) по договорам	Перечень конфиденциальной информации, к которой предоставляется доступ работникам Университета соответствующего структурного подразделения в соответствии с обязательством о неразглашении
			<ul style="list-style-type: none"> - 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
		Начальник управления экономики и финансов и его заместители	<ul style="list-style-type: none"> - штатная расстановка с указанием Ф.И.О. и оплаты труда работников; - информация, содержащаяся в регистрах внутренней финансовой отчетности; - договоры, контракты и соглашения, сведения об их исполнении
10	Научная деятельность	Отдел контрактных исследований	<ul style="list-style-type: none"> - сведения, касающиеся предмета договоров на выполнение научно-исследовательских и опытно-конструкторских работ, хода их исполнения и полученных результатов, если иное не предусмотрено договорами
11	Деятельность по цифровизации процессов Университета и обеспечению информационной безопасности	Начальник управления информационных технологий	<ol style="list-style-type: none"> 1. Информация по параметрам доступа (включая имена пользователей и пароли) к разрабатываемым и поддерживаемым управлением корпоративным информационным системам (далее - КИС) 2. Бизнес схемы, описывающие реализованные или планируемые к реализации процессы в КИС 3. Технические задания на модернизацию существующих и создание новых КИС 4. Реквизиты административного доступа к серверному, сетевому оборудованию, системам хранения данных, системам управления корпоративным информационным системам. 5. Сведения о производственно-технологических процессах, схемы и методики, дающие преимущество Университету.

№	Направления деятельности	Лица, уполномоченные на предоставление допуска и доступа к конфиденциальной информации работникам структурных подразделений, исполнителям (подрядчикам) по договорам	Перечень конфиденциальной информации, к которой предоставляется доступ работникам Университета соответствующего структурного подразделения в соответствии с обязательством о неразглашении
			<p>6. Реквизиты административного доступа к системам защиты информации.</p> <p>7. Сведения, содержащиеся в материалах, описывающих следующие направления обеспечения информационной безопасности, и которые могут быть использованы в дальнейшем для противоправных действий по нанесению ущерба Университету:</p> <ul style="list-style-type: none"> – 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.
12	Деятельность по правовому сопровождению	Начальник административно-правового управления в рамках своих должностных компетенций	<p>1. Информация, ставшая известной при подготовке материалов по результатам рассмотрения актов органов власти и служебных проверок, переписка с правоохранительными органами, материалы расследований и разбирательств;</p> <p>2. 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);</p> <p>3. Правовые позиции административно-правового управления по правовым вопросам, если они не являются общедоступными.</p>

№	Направления деятельности	Лица, уполномоченные на предоставление допуска и доступа к конфиденциальной информации работникам структурных подразделений, исполнителям (подрядчикам) по договорам	Перечень конфиденциальной информации, к которой предоставляется доступ работникам Университета соответствующего структурного подразделения в соответствии с обязательством о неразглашении
			4. Сведения о доходах, расходах, имуществе работников Университета, предоставляемые в рамках законодательства о противодействии коррупции (за исключением размещаемой публично информации).
13	Деятельность по работе с контингентом	Начальник учебно-методического управления, директора институтов, декан факультета, заведующие кафедрами	1. Документы по планированию образовательной деятельности, любые сведения по организации образовательной деятельности (за исключением общедоступной информации). 2. Сведения об основных показателях деятельности Университета, отчетность (за исключением размещаемой публично информации) 3. Документы конкурсного отбора абитуриентов.

СВЕДЕНИЯ О ДОКУМЕНТЕ

Документ разработан: Ефремова О.В., начальник отдела контрактных исследований; Гавриленко В.А., начальник управления информационных технологий; Смыслова А.Л., проректор по цифровой трансформации; Ячкуринских М.М., начальник административно-правового управления.

Документ введен взамен Положения о секретах производства (ноу-хау), коммерческой тайне и конфиденциальности информации Череповецкого государственного университета, утв. приказом ректора от 08.06.2021 № 05-02-36.

Сведения о внесении изменений в документ:

№ п/п	Реквизиты приказа ректора (номер, дата)			Номер раздела (подраздела, пункта, подпункта), в который внесены изменения
01	№		от	
02	№		от	
03	№		от	
04	№		от	
05	№		от	
06	№		от	
07	№		от	
08	№		от	
09	№		от	
10	№		от	