

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Бойко Валерий Леонидович
Должность: Ректор
Дата подписания: 08.09.2025 11:41:14
Уникальный программный ключ:
1ae60504b2c916e8fb686192f29d3bf1653db777



**Высшая Школа
Управления**

**Негосударственное образовательное частное учреждение высшего
образования «Высшая школа управления» (ЦКО)
(НОЧУ ВО «Высшая школа управления» (ЦКО))**

П Р И Н Я Т О

на заседании Ученого Совета
от «28» августа 2025 г.,
Протокол № 11

У Т В Е Р Ж Д А Ю

Ректор _____ В.Л. Бойко
«29» августа 2025 г.

Введено приказом Ректора
от «29» августа 2025 № 015/УМ/25

**Положение о коммерческой тайне и конфиденциальной информации
в Негосударственном образовательном частном учреждении высшего
образования «Высшая школа управления» (ЦКО)**

Москва
2025

1 Общие положения

1.1 Настоящее Положение о коммерческой тайне и конфиденциальной информации (далее - Положение) регулирует отношения, связанные с установлением, изменением режима конфиденциальности в отношении информации содержащей сведения отнесенные к коммерческой тайне, охраной ее конфиденциальности, доступом, обращением и передачей такой информации в целях обеспечения сохранения деятельности и интересов НОЧУ ВО «Высшая школа управления» и других участников регулируемых отношений, в том числе на рынке работ, услуг и предупреждения недобросовестной конкуренции.

1.2 Положение не распространяется на сведения, относящиеся в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства о государственной тайне и конфиденциальности информации.

1.3 Настоящее Положение разработано в соответствии с:

- Гражданским кодексом Российской Федерации;
- Федеральным законом «О коммерческой тайне»;
- Трудовым кодексом Российской Федерации;
- Федеральный закон "О персональных данных";
- иными федеральными законами и нормативными правовыми актами Российской Федерации.

1.4. Определения, употребляемые в настоящем Положении:

1.4.1. Конфиденциальная информация – сведения любого характера (учебно-методические, технические, интеллектуальные, экономические, организационные, образовательные, сведения в образовательных платформах и другие, имеющие коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых введен режим коммерческой тайны, в том числе: результаты образовательной и интеллектуальной деятельности; о способах осуществления профессиональной деятельности; сведения, содержащие информацию, ограниченную к передаче третьим лицам в силу закона и интереса Института.

1.4.2. Обладатель конфиденциальной информации – лицо, которое владеет информацией, составляющей коммерческую тайну (содержащей конфиденциальные сведения), на законном основании, ограничило доступ к этой информации и установило в отношении нее режим коммерческой тайны.

1.4.3. Разглашение конфиденциальной информации – действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известным третьим лицам без согласия руководства Института такой информации либо вопреки трудовому или гражданско-трудовому договору.

1.4.4. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая университету в связи с трудовыми отношениями и организацией образовательного процесса;

1.4.5. Информация для служебного пользования (служебная тайна) – режим конфиденциальной информации, которая стала известна работнику в связи с выполнением своих должностных обязанностей на основании трудового или иного договора;

1.4.6. Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

1.5. В целях охраны конфиденциальности информации Институт, может осуществлять следующие меры:

1.5.1. Ознакомление лица, доступ которого к информации, составляющей коммерческую тайну, необходим для выполнения им своих трудовых обязанностей, либо иных обязанностей, под расписку с перечнем информации, составляющей коммерческую тайну, обладателем которой является Работодатель и его контрагенты.

1.5.2. Ознакомление лица, которому представляется доступ к коммерческой тайне Института, под расписку с установленным режимом коммерческой тайны и с мерами ответственности за его нарушение.

1.6. В целях охраны конфиденциальной информации Института лицо, которому предоставляется доступ к коммерческой тайне обязано:

1.6.1. Выполнять установленный режим коммерческой тайны. Не разглашение документированной информации, представленной 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.

1.6.2. Не разглашать информацию, составляющую коммерческую тайну (содержащие конфиденциальные сведения), обладателями которой является Институт и его контрагенты и без их согласия не использовать эту информацию в личных целях.

1.6.3. Передать Институту:

- при прекращении или расторжении трудового договора – имеющиеся в пользовании работника материальные носители информации, содержащие информацию, составляющую коммерческую тайну, либо передать информацию отв. лицу, либо уничтожить такую информацию или удалить с личных материальных носителей под контролем Работодателя;

- при выходе из состава органов управления, имеющиеся в пользовании лица, которому предоставлялся доступ к коммерческой тайне, личные материальные носители информации должны быть либо уничтожены, либо удалена информация с этих материальных носителей под контролем Работодателя.

1.6.4. Об утрате или недостатке документов, содержащих закрытую информацию, а также ключей, печати, удостоверений, пропусков и т.п. немедленно сообщать Работодателю.

1.7. Ответственность за обеспечение режима коммерческой тайны и контроль за реализацией мер по его поддержке возлагается на лиц, получивших доступ к информации, составляющей коммерческую тайну.

1.8. Обязанность и ответственность лиц за обеспечение режима конфиденциальности информации, составляющей коммерческую тайну, предусматриваются в Соглашении о неразглашении коммерческой тайны (приложение 1).

1.9. Лица, получившие доступ к информации, составляющей коммерческую тайну, возмещают организации убытки, причиненные действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. Размер убытков определяется комиссией по интеллектуальной собственности (далее - Комиссия).

Обязанность возместить причиненные работодателю убытки, возникает, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей.

1.10. Ответственный за обеспечение конфиденциальности информации имеет право увольнять по статье за недоверие, работников Института, имеющих доступ к конфиденциальной информации и позволяющих распространение этой информации.

1.11. Конфиденциальная информация не может быть использована работниками Института в целях причинения имущественного, экономического, интеллектуального и морального вреда Институту.

1.12. Конфиденциальная информация (сведения), обращающаяся в документообороте и обрабатываемая в сфере информационных технологий, в зависимости от ее значимости и потенциальной опасности неправомерного использования относится информация (сведения), разглашение (утечка) которой может привести к нарушению экономической безопасности Института в целом, лишить его лидирующего положения на рынке, существенно снизить прибыль, сорвать реализацию стратегических планов, вызвать осложнения на отдельных направлениях деятельности Института, а также может снизить эффективность работы с контрагентами и клиентами, создать физическую угрозу безопасности объектов, имуществу и персоналу, привести к дополнительным материальным затратам.

Конфиденциальная информация (сведения), которая не может быть

отнесена к коммерческой тайне, но не должна быть общедоступной, так как предание ее огласке нанесет ущерб интересам Института, или доступ к которой должен быть ограничен в соответствии с требованиями действующего законодательства Российской Федерации.

1.13. Обработка и передача конфиденциальной информации с использованием средств вычислительной техники осуществляется с соблюдением требований коммерческой тайны.

2. Порядок оформления и прекращения допуска работников Института к конфиденциальной информации

2.1. Отдел кадров и юрист Института предупреждает работников об ответственности за неразглашение конфиденциальной информации, ставшей ему известной в связи с выполнением должностных обязанностей путём заключения с принимаемым работником договора о неразглашении конфиденциальной информации в отделе кадров и ознакомления под роспись с настоящим Положением.

2.2. Допуск работников к персональным данным определён положением «О персональных данных работников и обучающихся».

Допуск работника к конфиденциальной информации может быть прекращён в следующих случаях:

- прекращение трудового договора (независимо от причин прекращения);
- однократное нарушение работником взятых на себя обязательств, связанных с неразглашением и охраной конфиденциальной информации;

За разглашение конфиденциальной информации, а также нарушение порядка обращения с машинными носителями информации и документами, содержащими такую информацию, за нарушение режима защиты, обработки и порядка использования этой информации, работник может быть привлечен к дисциплинарной, административной и уголовной ответственности, предусмотренной действующим законодательством Российской Федерации.

3. Организационные мероприятия по охране конфиденциальной информации

3.1. Информационные ресурсы, содержащие конфиденциальную информацию, сформированные в процессе деятельности и выполнения должностных обязанностей работников управлений, отделов, кафедр и иных структурных подразделений Института, а также приобретенные на основании закона или договора, не могут быть использованы иначе как с разрешения Института или в установленных законом случаях.

Ответственность за организацию работ по защите конфиденциальной информации возлагается на руководителей структурных подразделений университета.

Руководители структурных подразделений университета обязаны принимать меры по защите конфиденциальной информации:

- ограничение доступа к конфиденциальной информации для посторонних лиц и работников университета, непосредственно не связанных с этими сведениями (И 15.003–2010 «О пропускном режиме на объектах университета»);

- организация надлежащего хранения физических носителей информации, таких как документация (И 20.011–2014 «О порядке обращения со служебной информацией ограниченного распространения в ЮЗГУ»), образцы техники, машиночитаемые носители;

- соблюдение установленных в университете правил работы с электронными устройствами и каналами хранения, обработки и передачи информации путем использования средств защиты информации от несанкционированного доступа (П 27.024-2014 «О корпоративной компьютерной сети ЮЗГУ»);

- неразглашение сведений, составляющих конфиденциальную информацию университета, в публикациях, докладах, документации, при экспонировании на выставках, в ходе организационно-технических переговоров, служебных и неслужебных разговоров и т.п.

Порядок обеспечения безопасности информационных ресурсов, содержащих конфиденциальную информацию, определён положением П 27.023-2014 «Об организации информационной безопасности в корпоративной компьютерной сети», устанавливающим требования к организационным, техническим, программным, криптографическим средствам и мерам по защите информации в процессе документооборота при работе исполнителей с конфиденциальными документами и сведениями, обработке информации в автоматизированных системах различного уровня и назначения, передаче её по каналам связи, при ведении конфиденциальных переговоров, как при непосредственном общении, так и по телефону и пр., сохранности оборудования и электронных носителей, печатных документов и пр.

ОБЯЗАННОСТИ РАБОТНИКОВ, ДОПУЩЕННЫХ К КОММЕРЧЕСКОЙ ТАЙНЕ И (ИЛИ) ИНОЙ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Работники Общества, допущенные к коммерческой тайне и (или) иной конфиденциальной информации, обязаны:

- 1) соблюдать установленный режим конфиденциальности;
- 2) знать и выполнять требования Положения и других нормативных документов Общества, регламентирующих вопросы обеспечения режима коммерческой тайны и порядка обращения с конфиденциальной информацией;
- 3) не разглашать конфиденциальную информацию, полученную в результате выполнения своих должностных обязанностей, обладателями которой являются Общество и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;
- 4) возместить Обществу убытки, причиненные Разглашением информации, составляющей коммерческую тайну и (или) иную конфиденциальную информацию, и (или) оплатить штраф, установленный соглашением (договором);
- 5) передать Обществу при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну;
- 6) соблюдать установленные в Обществе правила работы с документами, порядок их учета, хранения и уничтожения;
- 7) знакомиться только с теми документами и информацией, к которым получили допуск в силу своих должностных обязанностей;
- 8) во время работы с документами принимать меры к исключению возможности ознакомления с ними других лиц, не имеющих к ним прямого отношения;
- 9) пресекать действия других лиц, которые могут привести к Разглашению сведений, составляющих коммерческую тайну и (или) иную конфиденциальную информацию;

- 10) при составлении конфиденциальных документов ограничиваться минимальными, действительно необходимыми сведениями, составляющими коммерческую тайну;
 - 11) определять количество экземпляров документа в строгом соответствии со служебной необходимостью;
 - 12) документы и информацию, содержащие коммерческую тайну и находящиеся на исполнении, хранить в ограниченном доступе (выделенных сетевых папках/сетевых ресурсах Компаний Группы, офисах Компаний Группы, офисах обособленных структурных подразделений Компаний Группы);
 - 13) незамедлительно информировать руководителя структурного подразделения и руководителя Направления информационной безопасности о недостатке документов (отдельных листов), содержащих коммерческую тайну, ключей от сейфов (шкафов), кабинетов, о фактах обнаружения неучтенных конфиденциальных документов, о фактах несанкционированного доступа, а также о фактах интереса к сведениям, составляющим коммерческую тайну, лиц к ним не допущенных;
 - 14) при увольнении, переводе, убытии в отпуск или длительную командировку (более 1 месяца) передать документы (информацию для доступа) ответственному лицу в соответствии с внутренними нормативными документами Общества;
- 1.1. Дополнительно, в рамках контроля над соблюдением требований по обеспечению конфиденциальности, руководители подразделений обязаны:
- 1) контролировать процесс ознакомления подчинённых с требованиями внутренних нормативных документов Общества по вопросам обращения с конфиденциальной информацией;
 - 2) поддерживать надлежащее материально-техническое обеспечение деятельности в целях защиты конфиденциальной информации;
 - 3) регулировать допуск персонала к сведениям, составляющим коммерческую тайну и (или) иную конфиденциальную информацию;
 - 4) выявлять и пресекать попытки неправомерного использования, порчи, уничтожения или хищения носителей конфиденциальной информации;
 - 5) обеспечивать надежное хранение документов, содержащих сведения ограниченного доступа и находящихся в распоряжении подразделения;
 - 6) сообщать о выявленных попытках неправомерного

использования (включая Разглашение), порчи, уничтожения или хищения информации ограниченного доступа в Направление информационной безопасности.

1.2. При обработке конфиденциальной информации с использованием средств вычислительной и оргтехники работники обязаны:

- 1) соблюдать правила разграничения доступа к охраняемым данным, неукоснительно выполнять требования нормативных документов по организации доступа к информационным ресурсам, организации парольной и антивирусной защиты;
- 2) не разглашать свои индивидуальные учётные данные (логины и пароли) на доступ к компьютерным, Корпоративному portalу, сетевым и иным информационным ресурсам, выполнять рекомендации и требования администраторов систем и администраторов информационной безопасности;

- 3) не использовать (не загружать, не запускать и т.п.) для обработки конфиденциальной информации сторонние программные средства, не принятые для применения в Обществе;
- 4) при необходимости покинуть свое рабочее место и провести стандартные процедуры выхода из системы и отключения компьютера;
- 5) не допускать случаев передачи информации, составляющей коммерческую тайну, по незащищенным каналам передачи данных (в том числе, но не ограничиваясь – личная почта, мессенджеры и иные не корпоративные сервисы передачи данных и публичные сети;
- 6) немедленно информировать ответственного в рамках своей компетенции руководителя структурного подразделения и Направление информационной безопасности о фактах или возможности несанкционированного доступа к информации в локальной вычислительной сети (далее – «ЛВС») Общества.

1.3. Работникам, допущенным к коммерческой тайне и (или) иной конфиденциальной информации, запрещается:

- 1) снимать и изготавливать копии конфиденциальных документов, документов, отнесенных к категории коммерческой тайны (в том числе с электронных документов), делать из них выписки – если указанные действия не соответствуют целям правомерного раскрытия конфиденциальной информации или без разрешения руководителя структурного подразделения, ответственного за обеспечение режима коммерческой тайны или конфиденциальной информации на участке деятельности подразделения;
- 2) выносить за пределы офисов Общества документы и машинные носители с информацией, составляющей коммерческую тайну, и иными конфиденциальными сведениями без разрешения руководителя своего подразделения;
- 3) работать с документами и иными материалами, содержащими коммерческую тайну и (или) иную конфиденциальную информацию, вне офисов Общества;
- 4) обсуждать вопросы, содержащие коммерческую тайну, иные конфиденциальные сведения в присутствии посторонних лиц;
- 5) сообщать устно или письменно кому бы то ни было коммерческую тайну, иную конфиденциальную информацию, если это не обусловлено выполнением служебных обязанностей.

1.4. Кроме того, работникам Общества запрещается:

- 1) без согласования с Направлением информационной безопасности, оформленным на портале технической поддержки в разделе Безопасность, и руководителем структурного подразделения, ответственного за обеспечение режима коммерческой тайны или конфиденциальной информации на участке деятельности подразделения, подключать к компьютерам различного рода внешние устройства (включая, но не ограничиваясь - телефоны, внешние жесткие диски, флешки, модемы);
- 2) самостоятельно, без согласования с Направлением информационной безопасности, оформленным на Корпоративном портале, и руководителем подразделения, ответственного за обеспечение режима коммерческой тайны или конфиденциальной информации на участке деятельности подразделения, подключать (или допускать подключение) к ЛВС Общества компьютеры (в

том числе мобильные) представителей контрагентов и других организаций или физических лиц, прибывающих в Общество;

- 3) использовать для сохранения информации, составляющей коммерческую тайну, личные (не принадлежащие Обществу) компьютеры (в том числе мобильные - ноутбуки, электронные записные книжки, смартфоны, мобильные телефоны и другие мобильные цифровые (вычислительные) устройства).

2. ЗАЩИТА КОММЕРЧЕСКОЙ ТАЙНЫ ПРИ ОБРАБОТКЕ ИНФОРМАЦИИ НА СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

2.1. Сохранность конфиденциальной информации при ее обработке на СВТ и передаче по компьютерным сетям Общества обеспечивается осуществлением комплекса организационных, технических и программных мер защиты информации.

2.2. Обязательными условиями обработки конфиденциальной информации на СВТ являются:

- персонификация доступов в корпоративные системы и сервисы в соответствии с установленным порядком;
- разграничение полномочий доступа пользователей к информационным ресурсам, корпоративным системам и сервисам в соответствии с установленным порядком;
- обособленное хранение (в отдельных областях сетевых дисков, директориях, папках, файлах и т.п.) сведений, составляющих коммерческую тайну, с соблюдением принципа минимально необходимых прав доступа;
- резервирование информации;
- своевременное гарантированное уничтожение документов и проектов документов (включая уничтожение с машинных носителей информации), содержащих коммерческую тайну и иную конфиденциальную информацию;
- исключение несанкционированного доступа к информации, содержащей коммерческую тайну и иную конфиденциальную информацию в соответствии с установленными в Обществе правилами;

3. ТРЕБОВАНИЯ ПО ОБОРУДОВАНИЮ ПОМЕЩЕНИЙ И РАБОЧИХ МЕСТ

3.1. Входные двери (окна) помещений, в которых производится обработка и хранение документов, содержащих коммерческую тайну, должны иметь замки (запоры), гарантирующие надежное их закрытие.

3.2. Порядок использования ключей (механических, электронных) должен исключать несанкционированный доступ в эти помещения посторонних

Положение о коммерческой тайне и конфиденциальной информации

лиц.

- 3.3. Для хранения и работы с документами и информацией, содержащей конфиденциальную информацию и/или коммерческую тайну, работники обеспечиваются необходимой оргтехникой по запросам руководителей в принятом в Обществе порядке.

4. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ СТОРОННИМ ОРГАНИЗАЦИЯМ И ТРЕТЬИМ ЛИЦАМ

- 4.1. Предоставление информации о деятельности Общества органам государственной власти, иным государственным органам, органам местного самоуправления
-

осуществляется в порядке, установленном законодательством Российской Федерации, на основании мотивированного требования, подписанного уполномоченным должностным лицом и содержащего указание цели и правового основания затребования информации, составляющей коммерческую тайну и (или) иную конфиденциальную информацию, и срок предоставления этой информации, если иное не установлено федеральными законами.

- 4.2. Передача информации контрагентам (юридическим или физическим лицам) Общества осуществляется на основании договора в объеме и на условиях, которые предусмотрены договором.
- 4.3. Соглашение о неразглашении информации, определяющее условия конфиденциальности, срок их действия и порядок передачи коммерческой тайны, иной конфиденциальной информации, заключается как неотъемлемое приложение к договору на выполнение работ (оказание услуг, поставки и т.п.). Допускается условия обеспечения конфиденциальности оформлять отдельным разделом договора.
- 4.4. Если при подготовке к заключению договора необходимо ознакомление контрагента с коммерческой тайной или иными конфиденциальными сведениями Общества, соглашение о неразглашении информации заключается до передачи этих конфиденциальных сведений и заключения основного договора с последующим уточнением, при необходимости, условий конфиденциальности в соглашении о неразглашении информации при подписании основного договора. В этом случае соглашение о неразглашении информации (соглашение о конфиденциальности) заключается и оформляется отдельным документом в соответствии с порядком, установленным в Обществе для заключения договоров.
- 4.5. Право подписи от имени Общества соглашения о неразглашении информации предоставляется Исполнительному директору Общества на основании Устава, а также другим лицам – на основании доверенности, оформленной в установленном порядке.
- 4.6. Передача сторонним организациям и физическим лицам информации, составляющей коммерческую тайну контрагентов Общества, должна осуществляться с их письменного согласия, на основании соответствующих запросов или заключенных договоров (соглашений, контрактов).
- 4.7. Передача конфиденциальной информации может осуществляться на бумажных носителях, если их передача на иных носителях не предусмотрена действующим законодательством Российской Федерации либо условиями заключенных договоров. В случае, когда подлежащие передаче документы содержат конфиденциальную информацию, обязательно проставление на них соответствующего ограничительного грифа. На документах, содержащих информацию, составляющую коммерческую тайну, дополнительно указывается наименование обладателя информации и его местоположение.
- 4.8. Передача конфиденциальных сведений должна осуществляться, как правило, в электронном виде, либо на машинном носителе с сопроводительным письмом, если их передача на иных носителях не предусмотрена действующим законодательством Российской Федерации либо условиями заключенных договоров. В сопроводительном письме указываются перечень и ограничительный гриф отдельных файлов (информационных массивов), записанных на данном носителе.
- 4.9. Передача конфиденциальной информации сторонним организациям на машинных носителях, в том числе запись информации на машинные носители принимающей стороны, без согласования Исполнительного директора Общества или Уполномоченных лиц запрещается.
- 4.10. Для раскрытия (предоставления) третьим лицам конфиденциальной информации

необходимо последовательно выполнить следующие действия:

(i) заключить третьим лицом соглашение о неразглашении информации, либо

убедиться в наличии действующего на момент раскрытия соглашения о неразглашении информации, либо иной сделки, по условиям которой третье лицо приняло на себя обязательства о неразглашении.

(ii) в случае, если это требуется в соответствии с Положением (Приложение №4) - согласовать раскрытие с лицом, уполномоченным на предоставление согласия (запрета) на раскрытие конфиденциальной информации третьим лицам (далее – **«Уполномоченное лицо»**), в соответствии с пунктом 11.11 настоящего Положения, до раскрытия конфиденциальной информации третьему лицу.

Приказом Исполнительного директора Общества может быть определен круг лиц, на который не распространяются положения настоящего подпункта (ii) пункта 11.10 Положения, и (или) указание на это может быть предусмотрено в должностной инструкции работника Общества.

(iii) подготовить конфиденциальную информацию к раскрытию в порядке, предусмотренном настоящим разделом положения.

4.11. Согласование раскрытия (предоставления) осуществляется путем направления запроса Уполномоченному лицу на адреса электронной почты. Запрос должен содержать информацию о целях раскрытия коммерческой тайны и (или) конфиденциальной информации, кому необходимо раскрыть конфиденциальную информацию, объем и способы раскрытия информации. Согласование требуется только в случаях, прямо указанных в Приложении №4 к Положению.

Уполномоченное лицо, а также адрес электронной почты для направления запроса на предоставление согласия на раскрытие конфиденциальной информации третьим лицам, утверждаются приказом Исполнительного директора.

4.12. Раскрытие штатной структуры осуществляется только с предварительного согласования Директора по персоналу.

5. ОПУБЛИКОВАНИЕ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

5.1. Запрещается публикация материалов, содержащих коммерческую тайну и иные конфиденциальные сведения, в средствах массовой информации, включая сеть Интернет, а также использование их в публичных выступлениях до снятия в установленном порядке существующих ограничений.

5.2. Возможность открытого оглашения (публикации) сведений, составляющих коммерческую тайну, или иных конфиденциальных сведений, владельцем которых является Общество, определяется Исполнительным директором Общества.

Открытое оглашение (публикация) коммерческой тайны или иных конфиденциальных сведений, в отношении которых Общество не является владельцем (собственником), может осуществляться при наличии письменного согласия владельца (собственника) этой информации на ее открытое оглашение (публикацию), а также в иных случаях, предусмотренных действующим законодательством Российской Федерации.

5.3. В случае принятия такого решения и открытого оглашения (публикации) сведений:
- сведения утрачивают статус коммерческой тайны Общества (статус конфиденциальности), в отношении этих сведений утрачивает действие режим коммерческой тайны, установленный в Обществе Положением и другими локальными нормативными актами Общества;

- на документах, содержащих эти сведения, ограничительный гриф снимается;
- в отношении этих сведений утрачивается действие обязательства и условия конфиденциальности в действующих договорах (соглашениях, контрактах), заключенных ранее.

5.4. Появление в средствах массовой информации сведений, составляющих коммерческую

тайну Общества, и иных конфиденциальных сведений, в порядке, отличном от описанного в пункте 12.2 настоящего Положения, а также использование ноу-хау Общества другими юридическими и физическими лицами не означает выполнения по отношению к этим сведениям (информации) мероприятий, изложенных в пункте 12.3 настоящего Положения.

- 5.5. При публикации в средствах массовой информации, включая сеть Интернет, статей, касающихся деятельности Общества, работники – авторы статей обязаны соотносить используемый в публикациях материал с действующими в Обществе Перечнем коммерческой тайны и Перечнем конфиденциальной информации.
- 5.6. Работники, обнаружившие факт публикации в средствах массовой информации, включая сеть Интернет, а также использования в публичных выступлениях конфиденциальных сведений, в отношении которых в Обществе установлен режим коммерческой тайны, иной конфиденциальной информации обязаны сообщить об этом своему непосредственному руководителю.

6. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ИНФОРМАЦИИ (СВЕДЕНИЙ), СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, И ИНЫХ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ

- 6.1. Разглашение сведений, составляющих коммерческую тайну Общества, или Утрата документов, содержащих таковую, относится к числу грубых нарушений трудовых обязанностей.
- 6.2. За Разглашение сведений, составляющих коммерческую тайну Общества и его контрагентов, Утрату документов, содержащих такие сведения, а также за иные нарушения режима коммерческой тайны виновные лица несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.
- 6.3. За Разглашение конфиденциальных сведений, не составляющих коммерческую тайну Общества и его контрагентов, Утрату документов, содержащих такие сведения, а также за иные нарушение установленного в Обществе порядка учета, хранения, обращения с конфиденциальными документами и информацией, не содержащих коммерческой тайны, виновные несут предусмотренную действующим законодательством Российской Федерации ответственность.

7. ПРОВЕДЕНИЕ СЛУЖЕБНОГО РАССЛЕДОВАНИЯ ПО ФАКТАМ РАЗГЛАШЕНИЯ (УТРАТЫ) КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ

- 7.1. По фактам Разглашения (Утраты) сведений, составляющих коммерческую тайну, и иных конфиденциальных сведений проводится служебное расследование.

Служебное расследование может также назначаться по фактам грубого нарушения установленных нормативными документами правил обращения с конфиденциальной информацией.

Для проведения служебного расследования приказом Исполнительного директора Общества назначается комиссия в составе не менее трех человек.

Руководитель структурного подразделения, проверяемого по фактам Разглашения

(Утраты) сведений, составляющих коммерческую тайну, и иных конфиденциальных сведений принимает активное участие в обеспечении работы комиссии.

7.2. Комиссия, проводящая служебное расследование:

- выясняет обстоятельства, причины Разглашения сведений или Утраты документов, а также способствовавшие этому условия;
- устанавливает лиц, виновных в Разглашении сведений или Утрате документов;

- принимает меры к розыску утраченного документа или предотвращению негативных последствий Разглашения сведений;

- в обязательном порядке запрашивает от работника, в соответствии с частью 1 статьи 193 Трудового кодекса Российской Федерации письменное объяснение. Если по истечении 2 (двух) рабочих дней указанное объяснение работником не предоставлено, то комиссия составляет соответствующий акт;

- производит оценку (i) насколько тяжелым является совершенное работником нарушение; (ii) при каких обстоятельствах оно было совершено, являются ли уважительными причины его совершения; (iii) есть ли вина работника, а также каким было его поведение, как в целом он относится к труду.

7.3. Члены комиссии, проводящие служебное расследование, имеют право:

- производить осмотр помещений Общества (сейфов, столов, шкафов, и т.д.);
- проверять конфиденциальную документацию;
- опрашивать работников Общества, виновных в Утрате (Разглашении), а также других работников Общества, могущих оказать содействие в установлении обстоятельств происшедшего и получать от них письменные объяснения;
- привлекать работников других структурных подразделений, не заинтересованных в исходе дела, для проведения отдельных действий служебного расследования по согласованию с их руководителями.

7.4. Служебное расследование проводится в минимально короткий срок, но не более 10 (десяти) рабочих дней со дня назначения комиссии. В случаях, когда в течение данного срока утраченные документы не обнаружены, поиск их может быть прекращен.

В случае, если по результатам расследования работник будет признан виновным, дисциплинарное взыскание может быть применено не позднее 1 (одного) месяца со дня обнаружения проступка, не считая времени болезни работника, пребывания его в отпуске, а также времени, необходимого на учет мнения представительного органа работников (если такой создан в Обществе).

7.5. По результатам расследования составляется заключение, в котором отражаются следующие вопросы:

- основания для проведения расследования;
- описание проступка (нарушения), обстоятельств, обязанностей, которые нарушил работник (с указанием документов, где они были отражены);
- кто и в какие сроки проводил расследование;
- перечень и результаты осуществленных мероприятий;
- виновные лица;
- оценка тяжести совершенного нарушения;
- выявленные причины и условия, способствовавшие Разглашению (Утрате);
- выводы о наличии/отсутствии уважительности причин совершения проступка (нарушения);
- последствия допущенного работником проступка (нарушения), которые могут свидетельствовать о тяжести нарушения, т.е. Разглашения (Утраты) сведений, составляющих коммерческую тайну, и иных конфиденциальных сведений;
- выводы о негативных последствиях происшедшего для интересов Общества и предложения по их устранению;
- мнение о наличии в действиях виновного лица признаков административного правонарушения либо уголовно наказуемого деяния.

7.6. Заключение по результатам служебного расследования докладывается Исполнительному директору Общества для принятия решения о привлечении виновного к дисциплинарной/ гражданско-правовой/ административной/ уголовной

ответственности (о передаче материалов в правоохранительные или судебные органы), а также о мерах по устранению причин и возможных негативных последствий

происшедшего либо об отклонении материалов расследования.

8. ДЕЙСТВИЕ ВНЕСЕНИЯ ПОЛОЖЕНИЕ

ПОЛОЖЕНИЯ. ПОРЯДОК ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В

- 8.1. Настоящее Положение вступает в силу с даты утверждения его Советом директоров Общества.
- 8.2. Внесение изменений и дополнений в настоящее Положение, а также принятие Положения в новой редакции относится к компетенции Совета директоров Общества.
- 8.3. В случае, если отдельные нормы настоящего Положения вступят в противоречие с законодательством Российской Федерации и/или Уставом Общества, они утрачивают силу и применяются соответствующие нормы законодательства Российской Федерации и/или Устава Общества. Недействительность отдельных норм настоящего Положения не влечет недействительности других норм и Положения в целом.
- 8.4. Ограничительные грифы, нанесенные на материальные и электронные носители до вступления в силу настоящего Положения и указывающие на наличие в них информации, составляющей коммерческую тайну, сохраняют свое действие при условии, что меры по охране конфиденциальности указанной информации соответствуют требованиям законодательства Российской Федерации и настоящего Положения.

ПЕРЕЧЕНЬ ИНФОРМАЦИИ, ОТНЕСЕННОЙ К КАТЕГОРИИ КОММЕРЧЕСКОЙ ТАЙНЫ

1. Бюджет (в целом и любые сведения, составляющие его, действующие и недействующие версии).
2. Результаты аудиторских проверок (кроме аудиторского заключения в рамках обязательного аудита и размещенных в публичном доступе в соответствии с пунктом 5.1 Положения).
3. Финансовая отчетность Общества, включая отчетность по стандартам МСФО (кроме размещенной в публичном доступе в соответствии с пунктом 5.1 Положения).
4. Сведения, содержащиеся в финансово-экономических обоснованиях инвестиционных проектов.
5. Сведения о финансовых, правовых и других взаимоотношениях с аффилированными лицами, до официального опубликования соответствующей информации.
6. Информация о планируемой реорганизации, ликвидации, реструктуризации, до официального опубликования соответствующей информации.
7. Информация о планируемых крупных сделках, сделках с заинтересованностью, сделках, требующих одобрения в соответствии с положениями Устава Общества, иных сделках, выходящих за рамки обычной хозяйственной деятельности Общества, до официального

опубликования соответствующей информации.

8. Сведения о ведении переговоров с инвесторами и иными потенциальными партнерами (включая, но не ограничиваясь, сам факт ведения переговоров, результаты переговоров, предварительные договоренности и т.д.).
9. Сведения о планах и стратегии развития Общества, включая, но не ограничиваясь, сведениями о планах по расширению или свертыванию направлений деятельности и других коммерческих замыслах, сведениями о текущих и перспективных планах и программах привлечения финансовых ресурсов, информацией о выпуске на рынок новых услуг, а также планами по продвижению Общества (маркетинговые мероприятия).
10. База данных контрагентов Общества – заказчиков (лица, которые приобретают услуги/товары Общества) и перевозчиков (лица, привлекаемые Обществом для оказания услуг по перевозке грузов). База данных – это совокупность информации о перечне действующих/бывших/потенциальных контрагентов и контактов для связи с ними, лиц, принимающих решение и контактов связи с ними и иной систематизированной информации.
11. Условия взаиморасчетов с контрагентами (порядок, суммы (тарифы, цена договора), за исключением публичной информации, размещаемой/распространяемой Обществом в

качестве публичных прейскурантов/условий, коммерческих предложений и пр.

12. Политика предоставления скидок, информация об индивидуальных и эксклюзивных условиях работы с контрагентами.
13. Условия договоров с контрагентами – лизинговыми компаниями, страховыми компаниями, кредитными и финансовыми организациями, поставщиками транспортных средств (дилеры, изготовители и пр.).
14. Сведения о фактической себестоимости реализуемых товаров и услуг Общества.
15. Уровень и объем транспортно-технического обеспечения (статистическая информация в разрезе марки, модели, особенностей спецификации, стоимости транспортных средств)
16. Любая аналитическая и статистическая информация о деятельности Общества за любой период времени (количество покупателей, количество поставщиков, количество транзакций, количество претензий, количество ДТП, количество заявок на перевозку грузов и т.д., и т.п.), за исключением статистической информации блока управления персоналом (текучесть, гендерный состав, географические и демографические показатели, стаж работы, производительность, вовлеченность, комплектация и пр.).
17. Информация о платежной дисциплине Общества.
18. Информация о движениях по расчетным счетам Общества.
19. Информация об остатках денежных средств на расчетных счетах Общества.
20. Информация о дебиторской и кредиторской задолженности Общества и иных результатах финансовой деятельности Общества (кроме сведений, необходимых для проверки правильности исчисления и уплаты налогов и других обязательных платежей в государственную бюджетную систему Российской Федерации, размещенных в публичном доступе в соответствии с пунктом 5.1 Положения).
21. Информация о платежной дисциплине контрагентов Общества.
22. Результаты маркетинговых исследований, относящихся к деятельности Общества.
23. Информация об исковых заявлениях, поданных в отношении Общества или Обществом в отношении третьих лиц (кроме публичной информации, доступной в картотеке арбитражных судов и судов общей юрисдикции), включая, но не ограничиваясь, сам факт предъявления претензии, иска, информацию о сумме и основаниях требования.
24. Информация о претензиях, поданных в отношении Общества или Обществом в отношении третьих лиц (кроме публичной информации, доступной в картотеке арбитражных судов и судов общей юрисдикции), включая, но не ограничиваясь, сам факт предъявления претензии, информацию о сумме и основаниях требования.
25. Система и способы обеспечения общей (физической, технической) безопасности объектов инфраструктуры и Общества в целом.
26. Сведения о фактическом состоянии информационной безопасности информационных систем Общества.

27. Сведения об организации и результатах деятельности в сфере обеспечения экономической безопасности Общества.
28. Сведения о запланированных или проводимых мероприятиях по обеспечению информационной безопасности и о результатах их проведения (за исключением планов проверок).
29. Сведения, раскрывающие систему, методы, меры по защите информации, составляющей коммерческую тайну, и (или) иную конфиденциальную информацию от несанкционированных и (или) непреднамеренных воздействий, от утечки по техническим каналам.
30. Информация о служебных расследованиях Общества (основания проведения, результаты).
31. Информация о суммах страховых выплат по страховым случаям.
32. Принципы организации и система оптимизации бизнес-процессов Общества.
33. Информация о планируемых к регистрации объектах интеллектуальной собственности.
34. Служебные произведения Общества: задания на разработку, результаты работ (исходный код, включая, но не ограничиваясь, все промежуточные версии и входящие в них элементы вместе и по отдельности) - все, что относится к создаваемым объектам интеллектуальной собственности.
35. Исходный код программных продуктов, не являющихся служебными произведениями.
36. Сведения о внутренних бизнес-процессах в рамках проектов - система и способы управления, распределения задач, зоны ответственности, информация об уязвимостях и пр. – все, что не является общедоступным в силу раскрытия Обществом.
37. Условия соглашений между акционерами Общества, за исключением случаев раскрытия таких сведений в соответствии с требованием законодательства Российской Федерации, организатора торгов ценными бумагами.
38. Информация о любой Компании Группы в отношении сведений, указанных в пунктах 1-37 Перечня информации, отнесенной к категории коммерческой тайны настоящего Положения подлежит защите как информация, отнесенная к категории коммерческой тайны (при этом для целей настоящего пункта все ссылки на «Общество» в указанных пунктах следует читать как ссылки на соответствующее дочернее общество).

Приложение
№2 к Положению о коммерческой
тайне Акционерного общества
«МОНОПОЛИЯ», утвержденному
решением Совета
директоров АО
«МОНОПОЛИЯ» (Протокол №
60/2024 от 17.07.2024 г.)

**ПЕРЕЧЕНЬ ИНФОРМАЦИИ, ОТНЕСЕННОЙ К КАТЕГОРИИ ИНОЙ
КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ**

1. К сведениям, которые не составляют коммерческую тайну Общества, но имеют конфиденциальный характер, относятся:
 - i) информация служебного характера, которая не может быть отнесена к коммерческой тайне согласно требованиям законодательства:
 - статистические и отчетные документы, форма и содержание которых установлены нормативными актами органов государственной власти;
 - платежные документы;
 - сведения об исчислении и уплате налогов и обязательных платежей, о численности и составе работающих, их заработной плате и др.;
 - ii) служебные сведения, доступ к которым ограничен органами государственной власти;
 - iii) конфиденциальные сведения, защищаемые государством в иных режимах:
 - сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);
 - сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);
 - сведения, составляющие тайну следствия и судопроизводства;
 - сведения, защищаемые нормами патентного, авторско-правового и иного специального законодательства.
2. Информация о бенефициарах Общества (физических лицах), кроме размещенной в общем доступе в соответствии с пунктом 5.1 Положения.
3. Штатная структура Общества (совокупность информации о штатных единицах с указанием ФИО работников, их оклада)
4. Информация об аффилированных, взаимозависимых лицах, взаимосвязанных сторонах (кроме размещенной в публичном доступе в соответствии с пунктом 5.1 Положения)
5. Информация по уголовным делам, ведущимся в отношении работников Общества и связанных с их непосредственной деятельностью в Обществе (кроме публичной информации, доступной в картотеке судов общей юрисдикции).

6. Персональные данные сотрудников о заработной плате.
7. Персональные данные сотрудников Общества и персональные данные, предоставленные контрагентами Общества, и представленные/хранящиеся в форме базы данных –

совокупность информации с указанием ФИО и (или) контактных адресов электронной почты, и (или) номеров телефонов, и (или) иной информации, относящейся к персональным данным.

8. Информация об идентификационных данных (логин, пароль) для доступа к Информационным системам и иным хранилищам информации, доступ к которым ограничен (помимо прочего - к личным кабинетам Общества на сторонних информационных ресурсах) – данные Корпоративной учетной записи и Учетной записи для сторонних информационных ресурсов, а также о ключах электронной подписи (проверочные смс-коды и пр.), об идентификационных данных к банк-клиенту
9. Содержание телефонных разговоров с водителями транспортных средств.
10. Сводные данные мониторинга движения транспортных средств (систематизированная информация по какому-либо критерию).
11. Сведения, собираемые системой контроля доступа на территорию Общества.
12. Принципы организации электронного и бумажного документооборота.
13. Сведения, составляющие конфиденциальную информацию третьих лиц, переданные Обществу на договорной или иной основе (такая информация может быть отмечена как конфиденциальная, либо конфиденциальность может следовать из условий сделки между Обществом и таким третьим лицом).
14. Информация о требованиях к разрабатываемым программам для ЭВМ.
15. Сценарии автоматизации (скрипты).
16. Информация о планах развития существующих программ для ЭВМ (добавление/изменение функций) и разработки новых программ для ЭВМ.
17. Информация об интеграции программ для ЭВМ, принадлежащих/используемых Компаниями Группы, со сторонними программно-аппаратными комплексами.
18. Информация о метриках и их значениях применительно к разрабатываемым/эксплуатируемым программам для ЭВМ, данные Google-аналитики.
19. Аналитические данные о работе разрабатываемых/эксплуатируемых Обществом программ для ЭВМ - производительность, ошибки, сбои, информация о запросах на устранение нарушений, период недоступности и т.д.
20. Информация о подключенных провайдерах, адресах, IP, мощностях, дата-центрах, коммутации.
21. Условия работы с контрагентами-провайдерами услуг связи.
22. Информация о подключенных провайдерах, адресах, IP, мощностях, дата-центрах, коммутации.
23. Информация о поставщиках программных продуктов и об условиях лицензии на них.
24. Логические и физические схемы инфраструктуры, эксплуатируемого Обществом,

серверного и сетевого оборудования.

25. Информация о любой Компании Группы в отношении сведений, указанных в пунктах 1- 24 Перечня информации, отнесенной к категории иной конфиденциальной информации настоящего Положения подлежит защите как информация, отнесенная к категории коммерческой тайны (при этом для целей настоящего пункта все ссылки на «Общество» в указанных пунктах следует читать как ссылки на соответствующее дочернее общество).

УВЕДОМЛЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ: В настоящем письме содержатся сведения, составляющие коммерческую тайну и (или) иную конфиденциальную информацию.

Содержание данного электронного сообщения, включая любые приложения к нему, является конфиденциальным. Несанкционированное (без согласия правообладателя) использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых действий на основе этой информации, строго запрещено. Если Вы получили это сообщение по ошибке, пожалуйста, сообщите об этом отправителю по электронной почте и удалите это сообщение.

Раскрытие конфиденциальной информации в электронной форме возможно исключительно с корпоративного адреса электронной почты/ корпоративной учетной записи

ОБЯЗАТЕЛЬСТВО

Я, _____
(Фамилия, имя, отчество)

являясь работником СПбПУ, получил доступ к коммерческой тайне для выполнения работ по договорам НИР и ОКР, ознакомился с требованиями, установленными в СПбПУ по сохранению сведений, отнесенных к секрету производства,

о б я з у ю с ь:

1. В период работы в СПбПУ, а также в случае увольнения или перемены места работы не разглашать сведения, в отношении которых в СПбПУ введен режим коммерческой тайны, которые мне будут доверены или станут известными по работе.

2. Выполнять требования, установленные в СПБПУ по сохранению сведений, в отношении которых в СПБПУ введен режим коммерческой тайны.

Я предупрежден, что при нарушении мной п. 1 и п. 2 данного Обязательства как в период работы в СПБПУ так и после увольнения, я могу быть привлечен к дисциплинарной, административной или уголовной ответственности и взысканию нанесенного материального ущерба в соответствии с законодательством Российской Федерации.

(Фамилия и инициалы)

(подпись)

«__»_____202__г.