DIRECTUM-15000-3048595

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО «СПбПУ»)

ПРИКАЗ

10.10.2025 № 2878

Об утверждении Положения об организации защиты конфиденциальной информации в ФГАОУ ВО «СПбПУ»

В целях упорядочения обращения в ФГАОУ ВО «СПбПУ» с конфиденциальной информацией,

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Положение об организации защиты конфиденциальной информации в ФГАОУ ВО «СПбПУ» (далее – Положение) (Приложение № 1).
2. Руководителям структурных подразделений организовать изучение Положения работниками и обеспечить строгое соблюдение его требований.
3. К работе с конфиденциальной информацией в ФГАОУ ВО «СПбПУ» допускать только работников ФГАОУ ВО «СПбПУ», включенных в перечень, утверждаемый соответствующим обладателем конфиденциальной информации, прошедших предварительный инструктаж по работе с конфиденциальной информацией и ознакомленных с Положением.
4. Признать утратившими силу приказы от 03.04.2007 №148 «О запрете обработки конфиденциальной информации на неаттестованных средствах и системах информатизации в ГОУ «СПбГПУ»» и от 03.04.2007 №149 «Об организации защиты конфиденциальной информации в ГОУ «СПбГПУ»».
5. Контроль за исполнением приказа возложить на проректора по информационным технологиям и цифровой трансформации Лямина А.В.

Первый проректор В.В. Сергеев

DIRECTUM-15000-3048595

Проект вносит	Согласовано
А.Ю. Синицын (07.10.2025 10:44:12)	Е.М. Лимонова (07.10.2025 11:25:11) И.Г. Кадиев (07.10.2025 11:33:19) В.М. Крундышев (07.10.2025 16:16:43) А.В. Лямин (07.10.2025 17:18:38) Е.О. Шевчук (09.10.2025 16:43:59) _____ _____

Приложение
УТВЕРЖДЕНО
приказом ФГАОУ ВО «СПбПУ»
от 10.10.2025 № 2878

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»

ПОЛИТЕХ
Санкт-Петербургский политехнический университет Петра Великого

ПОЛОЖЕНИЕ
об организации защиты конфиденциальной информации в ФГАОУ ВО «СПбПУ»

Санкт-Петербург
2025

Содержание

1. Общие положения

1.1. Настоящее Положение устанавливает порядок обращения с конфиденциальной информацией, ограничения доступа к конфиденциальной информации, регулирует отношения по использованию конфиденциальной информации, определяет перечень сведений, составляющих конфиденциальную информацию федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (далее - СПбПУ), в соответствии с требованиями:

- Конституции Российской Федерации;
- Гражданского кодекса Российской Федерации;
- Федерального закона от 29.07.2004 №98-ФЗ «О коммерческой тайне»;
- Федерального закона от 07.07.2003 №126-ФЗ «О связи»;
- Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- Указа Президента Российской Федерации от 06.03.1997 №188 «Об утверждении Перечня сведений конфиденциального характера»;
- Указа Президента Российской Федерации от 05.12.2016 №646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
- Указа Президента Российской Федерации от 02.07.2021 №400 «О Стратегии национальной безопасности Российской Федерации»;
- Указа Президента Российской Федерации от 16.08.2004 №1085 «Вопросы Федеральной службы по техническому и экспортному контролю»;
- Постановления Правительства Российской Федерации от 21.11.2011 №957 «Об организации лицензирования отдельных видов деятельности»;
- Постановления Правительства Российской Федерации от 03.11.1994 №1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»;
- Постановления Правительства Российской Федерации от 03.02.2012 №79 «О лицензировании деятельности по технической защите конфиденциальной информации»;
- Решения Гостехкомиссии России и ФАПСИ от 27.04.1994 №10 «Положение о государственном лицензировании деятельности в области защиты информации»;
- Решения Коллегии Гостехкомиссии России №7.2/02.03.2001, утвержденного приказом Гостехкомиссии России от 30.08.2002 №282 «Специальные требования и рекомендации по технической защите конфиденциальной информации» (далее - СТР-К);

− Положения по аттестации объектов информатизации по требованиям безопасности информации (утв. председателем Гостехкомиссии России 25.11.1994);

− Методического документа «Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014);

− Приказа ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее - приказ ФСТЭК № 17);

− Приказа ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;

− Инструкции о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки Российской Федерации (утв. Приказом Министерства образования и науки Российской Федерации от 30.12.2010 №2233);

− Приказа Министерства науки и высшего образования Российской Федерации от 13.06.2023 №598 «Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве науки и высшего образования Российской Федерации и организациях, подведомственных Министерству науки и высшего образования Российской Федерации» (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки "Для служебного пользования" с носителей информации ограниченного распространения»);

− Устава СПбПУ.

1.2. Основные понятия, используемые в настоящем Положении:

1.2.1. Конфиденциальная информация - информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну. К конфиденциальной информации относятся любые сведения, доступ к которым ограничен законодательством и настоящим Положением: персональные данные, информация, составляющая коммерческую и служебную тайну.

1.2.2. Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

1.2.3. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Персональные данные, обрабатываемые в СПбПУ, относятся к сведениям, составляющим конфиденциальную информацию.

1.2.4. Коммерческая тайна - режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

1.2.5. Служебная тайна - режим конфиденциальности в отношении к информации, которая защищается законом и является собственностью органов государственного и муниципального управления, государственных учреждений и предприятий. Доступ к служебной тайне ограничивается федеральными законами или в силу служебной необходимости. На документах и носителях информации (в необходимых случаях и на их проектах), содержащих служебную тайну, проставляется пометка «Для служебного пользования».

1.2.6. Контрагент - сторона гражданско-правового договора, которой СПбПУ передала конфиденциальную информацию.

1.2.7. Передача конфиденциальной информации контрагенту - передача информации на основании договора (соглашения) в объеме и на условиях, которые предусмотрены договором (соглашением), включая условие о принятии контрагентом установленных договором (соглашением) мер по охране ее конфиденциальности.

1.2.8. Передача конфиденциальной информации от одного работника СПбПУ другому - передача информации на основании разрешения должностного лица, в соответствии с разделом 4 настоящего Положения и инструкцией по конфиденциальному делопроизводству в ФГАО ВО «СПбПУ».

1.2.9. Предоставление конфиденциальной информации - передача конфиденциальной информации, зафиксированной на материальном носителе, органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

1.2.10. 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 СПбПУ, либо вопреки трудовому или гражданско-правовому договору.

1.3. Меры по охране конфиденциальности информации, принимаемые СПбПУ, включают в себя:

1.3.1. Определение перечня сведений, составляющих конфиденциальную информацию ФГАОУ ВО «СПбПУ».

1.3.2. Ограничение доступа к конфиденциальной информации путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

1.3.3. Учет лиц, получивших доступ к конфиденциальной информации, и (или) лиц, которым такая информация была предоставлена или передана.

1.3.4. Регулирование отношений по использованию конфиденциальной информации работниками СПбПУ на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров.

1.3.5. Нанесение на материальные носители, содержащие конфиденциальную информацию, грифа о конфиденциальности («Конфиденциально», либо «Коммерческая тайна», «Для служебного пользования»), в соответствии с настоящим Положением и действующими инструкциями.

1.3.6. Применение информационных технологий с ограничением программной среды, регистрацией событий безопасности, антивирусной защитой, обнаружением(предотвращением) вторжений, контролем(анализом) защищенности, обеспечением целостности информационных систем.

1.4. Режим конфиденциальности считается установленным после принятия СПбПУ в отношении определенной информации мер, указанных в пункте 1.3 настоящего Положения.

1.5. Наряду с мерами, указанными в пункте 1.3 настоящего Положения, СПбПУ вправе применять при необходимости средства и методы технической защиты конфиденциальной информации, а также другие не противоречащие законодательству Российской Федерации меры.

1.6. Помещения, в которых хранятся документы, издания и другие носители информации, содержащие конфиденциальную информацию, а также средства вычислительной техники, предназначенные для обработки конфиденциальной информации, должны иметь охранную сигнализацию с выводом информации на пост охраны СПбПУ.

1.7. Неотъемлемой частью договора на выполнение научно-исследовательских, опытно-конструкторских работ и т.п., в котором отражены требования по обеспечению технической защиты конфиденциальной информации, должно быть соглашение о конфиденциальности (соглашение о неразглашении конфиденциальной информации), а также предусмотрены расходы на финансирование всех мероприятий по защите конфиденциальной информации.

1.8. По согласованию с проректором по информационным технологиям и цифровой трансформации проректоры, директора институтов, департаментов и центров, начальники управлений, отделов, служб назначают лиц, ответственных за учет, хранение, передачу, уничтожение, оформление и т.п. документов и других материальных носителей конфиденциальной информации, а также, в случае использования средств вычислительной техники для обработки конфиденциальной информации, администраторов по обеспечению безопасности информации.

1.9. Ответственность за выполнение требований по защите конфиденциальной информации в структурных подразделениях СПбПУ, установленных настоящим Положением, возлагается на проректоров по направлениям деятельности, на начальников управлений, руководителей департаментов и иных структурных подразделений прямого подчинения.

1.10. Организация работ по защите конфиденциальной информации, в соответствии с требованиями указанными в настоящем Положении, возлагается на руководителей структурных подразделений.

1.11. Мероприятия по защите конфиденциальной информации обеспечиваются отделом защиты конфиденциальной информации под контролем проректора по информационным технологиям и цифровой трансформации.

1.12. Ответственность за защиту конфиденциальной информации должна быть включена в должностные инструкции работников СПбПУ, включая

ответственность за выполнение требований информационной безопасности, за ресурсы, процессы и мероприятия по обеспечению безопасности.

1.13. За разглашение конфиденциальной информации, а также нарушение порядка обращения с носителями, содержащими такую информацию, работник СПбПУ может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

1.14. Отношения между работником и работодателем (СПбПУ), ответственность за нарушение в области защиты конфиденциальной информации регулируются, прежде всего, Трудовым кодексом Российской Федерации. В определенных случаях возможно применение положений Кодекса об административных правонарушениях и Уголовного кодекса.

2. Виды конфиденциальной информации СПбПУ

2.1. К конфиденциальной информации СПбПУ относятся:
- персональные данные;
- коммерческая тайна;
- служебная тайна.

2.2. Состав и категории сведений, которые относятся к тому или иному виду конфиденциальной информации, указан в Перечне сведений, составляющих конфиденциальную информацию ФГАОУ ВО «СПбПУ» (Приложение №1).

3. Права и обязанности СПбПУ в области защиты конфиденциальной информации

3.1. СПбПУ имеет право:

3.1.1. Устанавливать, изменять, отменять в письменной форме режим конфиденциальности в соответствии с законодательством Российской Федерации, настоящим Положением и гражданско-правовыми договорами.

3.1.2. Использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации.

3.1.3. Передавать информацию контрагентам по договору или на ином установленном законом основании.

3.1.4. Разрешать или ограничивать доступ к конфиденциальной информации, определять порядок и условия доступа к этой информации.

3.1.5. Осуществлять иные действия с информацией или разрешать осуществление таких действий в соответствии с требованиями законодательства Российской Федерации.

3.1.6. Требовать от юридических лиц, физических лиц, получивших доступ к конфиденциальной информации, органов государственной власти, иных государственных органов, органов местного самоуправления, которым

предоставлена информация, соблюдения обязанностей по охране ее конфиденциальности.

3.1.7. Требовать от лиц, получивших доступ к конфиденциальной информации, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации.

3.1.8. Защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами конфиденциальной информации, в том числе требовать возмещения убытков, причиненных в связи с нарушением ее прав.

3.2. Обязанности СПбПУ:

3.2.1. Соблюдать права и законные интересы иных лиц.

3.2.2. Принимать меры по защите конфиденциальной информации.

3.2.3. Ограничивать доступ к конфиденциальной информации в соответствии с требованиями законодательства Российской Федерации.

3.2.4. Предоставлять на безвозмездной основе сведения, составляющие конфиденциальную информацию СПбПУ, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления. Мотивированное требование должно быть подписано уполномоченным должностным лицом, содержать указание цели и правового основания затребования информации, составляющей коммерческую тайну, и срок предоставления этой информации, если иное не установлено федеральными законами.

3.2.5. Предоставлять конфиденциальную информацию по запросу судов, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации.

4. Права и обязанности работников СПбПУ в области защиты конфиденциальной информации

4.1. Обязательным условием приема на работу в СПбПУ должно быть подписание обязательства о неразглашении информации ограниченного доступа и соблюдении конфиденциальности персональных данных (далее - Обязательство), в котором указываются требования по защите конфиденциальной информации, предъявляемые к работнику, и ответственность за нарушения, связанные с разглашением конфиденциальной информации. Обязательство разрабатывается в соответствии с настоящим Положением и хранится после подписания в личном деле работника.

4.2. Работники СПбПУ обеспечиваются сведениями, составляющими конфиденциальную информацию, в объеме, необходимом для качественного и своевременного выполнения порученных им работ. Ознакомление работников СПбПУ с конфиденциальной информацией, не имеющей отношения к выполняемой ими работе, запрещается.

4.3. Для получения разрешения на выполнение работ, связанных со сведениями, составляющими конфиденциальную информацию, работники СПбПУ обязаны принять на себя обязательства о соблюдении установленного в СПбПУ порядка обращения с указанными сведениями и их носителями.

4.4. Работники СПбПУ обязаны хранить материальные носители конфиденциальной информации в условиях, исключающих возможность доступа к ним посторонних лиц.

4.5. Работники, допущенные к работам, изделиям, носителям конфиденциальной информации, обязаны немедленно сообщить руководителю структурного подразделения об утрате, недостаче материальных носителей конфиденциальной информации.

5. Права и обязанности должностных лиц СПбПУ, осуществляющих мероприятия по защите конфиденциальной информации

5.1. Состав должностных лиц, ответственных за защиту конфиденциальной информации в СПбПУ, включая перечень решаемых ими задач, определяется руководителями структурных подразделений СПбПУ.

5.2. Должностными лицами, ответственными за организацию и осуществление работ по защите конфиденциальной информации в СПбПУ, являются:

- ректор;
- проректор по информационным технологиям и цифровой трансформации;
- руководитель Управления информационной безопасности;
- начальник отдела защиты конфиденциальной информации;
- руководители структурных подразделений, в которых проводятся работы с конфиденциальной информацией.

5.3. Ректор:

- определяет организационно-штатную структуру СПбПУ по защите конфиденциальной информации, основные задачи структуры, назначает должностных лиц, ответственных за организацию защиты конфиденциальной информации;
- утверждает документы СПбПУ по защите конфиденциальной информации;
- принимает решения о финансировании мероприятий по защите конфиденциальной информации в СПбПУ;
- принимает решения о прекращении работ на объектах информатизации в случае выявления нарушений по защите конфиденциальной информации, а также о возобновлении выполнения работ после их устранения.

5.4. Проректор по информационным технологиям и цифровой трансформации:

- утверждает годовое и перспективное планирование мероприятий по защите конфиденциальной информации в СПбПУ;

− утверждает перечень планируемых и реализуемых работ по защите конфиденциальной информации в структурных подразделениях СПбПУ;

− согласовывает приказы о назначении ответственных за обеспечение защиты конфиденциальной информации в структурных подразделениях СПбПУ;

− осуществляет руководство деятельностью руководителя Управления информационной безопасности;

− проводит совещания с руководящим составом СПбПУ по вопросам защиты конфиденциальной информации;

− оценивает эффективность принимаемых мер защиты конфиденциальной информации.

5.5. Руководитель Управления информационной безопасности:

− организует деятельность по комплексной безопасности, включая защиту конфиденциальной информации;

− осуществляет руководство деятельностью начальника отдела защиты конфиденциальной информации;

− организует разработку необходимых организационно-технических мероприятий по защите конфиденциальной информации в СПбПУ;

− проводит совещания с руководящим составом СПбПУ по вопросам защиты конфиденциальной информации;

− согласовывает годовое и перспективное планирование мероприятий по защите конфиденциальной информации в СПбПУ;

− оценивает эффективность принимаемых мер защиты конфиденциальной информации и организует работы по устранению выявленных недостатков.

5.6. Начальник отдела защиты конфиденциальной информации:

− осуществляет формирование целей, приоритетов и ограничений систем защиты конфиденциальной информации в СПбПУ, в том числе их изменение по мере изменения внешних условий и внутренних потребностей, включая требования уполномоченных федеральных органов исполнительной власти;

− осуществляет формирование целей, приоритетов, обязанностей и полномочий персонала, обслуживающего средства и системы защиты конфиденциальной информации в СПбПУ;

− определяет объекты информатизации в СПбПУ, подлежащие защите, возможные технические каналы утечки конфиденциальной информации и несанкционированного доступа к ней;

− проводит анализ внутренних и внешних угроз несанкционированного доступа к конфиденциальной информации в СПбПУ;

− распределяет и готовит предложения по распределению обязанностей и полномочий персонала, обслуживающего средства и системы защиты конфиденциальной информации в СПбПУ;

− разрабатывает предложения по профессиональному развитию персонала, обслуживающего средства и системы защиты конфиденциальной информации в СПбПУ;

− осуществляет подготовку планов по развитию, модернизации систем защиты конфиденциальной информации в СПбПУ, формирование требований к отдельным элементам и системам в целом;

− осуществляет организацию и контроль исполнения работ по развитию, модернизации системы защиты конфиденциальной информации в СПбПУ;

− выявляет нарушения в технологии обработки конфиденциальной информации в СПбПУ;

− проверяет правильность функционирования систем разграничения доступа к конфиденциальной информации, наличие средств защиты конфиденциальной информации в СПбПУ, их качество и достаточность;

− организует документальное оформление проводимых защитных мероприятий, при работе с конфиденциальной информацией, готовит предложения по совершенствованию и внедрению средств защиты конфиденциальной информации на объектах информатизации в СПбПУ;

− принимает участие в работе по планированию мероприятий по защите конфиденциальной информации в структурных подразделениях СПбПУ;

− оказывает методическую помощь руководителям структурных подразделений СПбПУ в проведении работ по защите конфиденциальной информации;

− согласовывает перечень планируемых и реализуемых работ по защите конфиденциальной информации в структурных подразделениях СПбПУ;

− определяет необходимый состав, особенности размещения и функциональные возможности программных, программно-аппаратных (в том числе криптографических) средств, технических средств и систем защиты конфиденциальной информации в СПбПУ;

− организует приобретение средств и систем защиты конфиденциальной информации, включая их предварительные и приемочные испытания, опытную эксплуатацию в СПбПУ;

− организует проведение монтажа и настройки программных, программно-аппаратных (в том числе криптографических) средств, технических средств и систем защиты конфиденциальной информации в СПбПУ;

− организует установку и настройку программного обеспечения, необходимого для управления системами защиты конфиденциальной информации в СПбПУ;

− организует использование средств анализа функциональности средств и систем защиты конфиденциальной информации в СПбПУ;

− организует проверки уровня квалификации персонала, обслуживающего средства и системы защиты конфиденциальной информации в СПбПУ;

− проводит отдельные мероприятия в рамках проведения работ по аттестации объектов информатизации в СПбПУ на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну;

− контролирует целостность программных, программно-аппаратных (в том числе криптографических) средств, технических средств и систем защиты конфиденциальной информации в СПбПУ;

− контролирует соответствие параметров систем защиты конфиденциальной информации установленным требованиям, обеспечение своевременной корректировки настроек систем защиты конфиденциальной информации, в целях реагирования на выявленные нарушения в СПбПУ;

− контролирует исполнение требований инструкций и регламентов по эксплуатации средств и систем защиты конфиденциальной информации, настоящего Положения работниками СПбПУ и проводит плановые (не реже одного раза в год) и внеплановые (по мере необходимости) проверки в структурных подразделениях СПбПУ;

− составляет отчеты по результатам проверок, в том числе о выявлении инцидентов, которые могут привести к сбоям, нарушению функционирования или возникновению угроз безопасности конфиденциальной информации, циркулирующей в СПбПУ;

− незамедлительно докладывает руководителю Управления информационной безопасности о выявленных нарушениях установленных требований, а также о невозможности обеспечения необходимых условий по защите конфиденциальной информации на объектах информатизации СПбПУ;

− отчитывается перед руководителем Управления информационной безопасности о выполнении мероприятий по защите конфиденциальной информации на объектах информатизации СПбПУ.

5.7. Руководители структурных подразделений, в которых проводятся работы с конфиденциальной информацией:

− организуют и проводят работы по защите конфиденциальной информации, находящейся в подчиненных подразделениях;

− организуют работу с конфиденциальной информацией, включая учет работников, допущенных к конфиденциальной информации, находящейся в подчиненных подразделениях;

− представляют проректору по информационным технологиям и цифровой трансформации согласованный с начальником отдела защиты конфиденциальной информации перечень планируемых и реализуемых работ по защите конфиденциальной информации;

− принимают меры по сохранности конфиденциальной информации, находящейся в подчиненных подразделениях, включая обеспечение ее нахождения в недоступном для третьих лиц месте (в специальных помещениях, запирающихся шкафах, сейфах, защищенных электронных хранилищах и т.д.);

− определяют перечень помещений, выделенных для проведения конфиденциальных мероприятий (совещаний, переговоров и т.п.) и технических средств (основных и вспомогательных), необходимых для осуществления основной деятельности в подразделении;

− организуют работы и принимают участие в аттестации объектов информатизации, находящихся в заведовании, на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну, включая учет, категорирование, проведение специсследований и специальных проверок технических средств объекта

информатизации, а также мероприятия по предотвращению несанкционированного доступа к конфиденциальной информации;

− согласовывают с начальником отдела защиты конфиденциальной информации установку на аттестованном объекте информатизации средств вычислительной техники и средств радиосвязи;

− контролируют установку средств защиты конфиденциальной информации и осуществляют их эксплуатацию в подчиненных подразделениях;

− контролируют исполнение настоящего Положения работниками подразделения и проводят плановые (не реже одного раза в полгода) и внеплановые (по мере необходимости) проверки в подразделении;

− разрабатывают совместно с начальником отдела защиты конфиденциальной информации эксплуатационную документацию по защите конфиденциальной информации на объекте информатизации.

6. Состав информации, которая не может быть отнесена к конфиденциальной и доступ не может быть ограничен

6.1. Нормативно-правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, а также устанавливающие правовое положение организаций и полномочия государственных органов, органов местного самоуправления.

6.2. Информация о состоянии окружающей среды.

6.3. Информация об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну).

6.4. Информация, накапливаемая в открытых фондах библиотек, музеев, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией.

6.5. Информация, содержащаяся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством Российской Федерации).

6.6. Иная информация, недопустимость ограничения доступа к которой установлена федеральными законами.

7. Порядок обращения со сведениями, составляющими персональные данные

7.1. Порядок обращения в СПбПУ со сведениями, составляющими персональные данные, регламентируется Положением о персональных данных ФГАОУ ВО «СПбПУ» (приказ ректора от 29.11.2024 № 3136 «Об утверждении Положения об обработке персональных данных в ФГАОУ ВО «СПбПУ»»).

8. Порядок обращения со сведениями, составляющими коммерческую тайну

8.1. В соответствии с действующим законодательством (ст.10 и 11 Федерального закона от 29.07.2004 №98-ФЗ «О коммерческой тайне»), обладатель секрета производства (ноу-хау) должен принять меры по охране конфиденциальности этих сведений путем введения режима коммерческой тайны.

8.2. В соответствии с п. 1 ст. 1465 Гражданского кодекса Российской Федерации секретом производства (ноу-хау) признаются сведения любого характера (производственные, технические, экономические, организационные и другие) о результатах интеллектуальной деятельности в научно-технической сфере и о способах осуществления профессиональной деятельности, имеющие действительную или потенциальную коммерческую ценность вследствие неизвестности их третьим лицам, если к таким сведениям у третьих лиц нет свободного доступа на законном основании и обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны.

8.3. Для секрета производства (ноу-хау) действующее законодательство не предусматривает выдачу документа, подтверждающего исключительное право обладателя секрета производства на его использование.

8.4. Исключительное право на секрет производства (ноу-хау) действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих его содержание (ст.1467 Гражданского Кодекса Российской Федерации). С момента утраты конфиденциальности соответствующих сведений исключительное право на секрет производства прекращается у всех правообладателей.

8.5. Право на отнесение информации к сведениям, составляющим коммерческую тайну, и на определение перечня и состава таких сведений принадлежит СПбПУ с учетом положений Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

8.6. Информация, составляющая коммерческую тайну, может быть получена от СПбПУ или передана СПбПУ на основании договора, соглашения о конфиденциальности и другими законными способами.

8.7. Информация, составляющая коммерческую тайну СПбПУ, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых СПбПУ мер по охране конфиденциальности этой информации, а также, если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является СПбПУ, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

8.8. Режим коммерческой тайны не может быть установлен в отношении следующих сведений:

8.8.1. Содержащихся в учредительных документах СПбПУ, документах, подтверждающих факт внесения записей об СПбПУ в соответствующие государственные реестры.

8.8.2. Содержащихся в документах, дающих право СПбПУ на осуществление предпринимательской деятельности.

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

8.8.4. О численности, о составе работников СПбПУ, 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 в СПбПУ.

8.8.5. О задолженности СПбПУ по выплате заработной платы и по иным социальным выплатам.

8.8.6. О нарушениях законодательства Российской Федерации и фактах привлечения СПбПУ и его должностных лиц к ответственности за совершение этих нарушений.

8.8.7. Обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена федеральными законами.

8.9. Отнесение информации к сведениям, составляющим коммерческую тайну СПбПУ, установление режима коммерческой тайны и нанесение грифа «Коммерческая тайна», осуществляются на основании решения Научно-технического совета СПбПУ (далее - НТС), приказов и распоряжений ректора или проректоров по направлению деятельности.

8.10. На основе анализа информации НТС принимает решения об отнесении сведений к категории защищаемой информации либо исключении сведений из указанной категории. Порядок организации работы НТС регламентируется внутренними положениями СПбПУ. Признание результатов интеллектуальной деятельности творческого коллектива или автора в качестве секрета производства осуществляется решением НТС по представлению Комиссии по управлению интеллектуальной собственности на основании заключения ученого совета института, работниками которого создан РИД. Результатом работы НТС является:

- заключение о целесообразности отнесения секрета производства (ноу-хау) к коммерческой тайне;
- приказ об установлении режима коммерческой тайны и нанесении грифа «Коммерческая тайна» (далее - «КТ») на все документы, составляющие коммерческую тайну.

8.11. Документы передаются на хранение в структурное подразделение Университета, ответственное за оформление и учет результатов интеллектуальной деятельности (РИД), принадлежащих СПбПУ.

8.12. Руководитель структурного подразделения, в котором создан секрет производства (ноу-хау), подготавливает список работников, имеющих доступ к

работе с документами, имеющими гриф «КТ». Список утверждается проректором по направлению деятельности и хранится вместе с указанными документами.

8.13. Работники, допущенные к работе с документами, в отношении которых установлен режим коммерческой тайны, подписывают обязательство по соблюдению установленного режима «КТ».

8.14. Документы, содержащие коммерческую тайну, должны иметь титульный лист со следующими реквизитами: наименование, количество листов в одном экземпляре, количество экземпляров, наименование правообладателя. Материалы вместе с титульным листом должны быть сброшюрованы и прошиты, страницы пронумерованы. На листе-наклейке, скрепляющем концы прошивочной нити на обороте последнего листа, указывается количество прошитых и пронумерованных страниц, ставится ФИО и подпись исполнителя.

8.15. Информация, в отношении которой не введен режим коммерческой тайны, не может быть отнесена к коммерческой тайне.

8.16. Обязанности по регистрации, учету, ведению реестра документов с грифом «КТ» и передаче на хранение в Архив СПбПУ или в Центр интеллектуальной собственности и трансфера технологий СПбПУ возлагаются на ответственных исполнителей в структурных подразделениях СПбПУ, назначенных приказом.

8.17. Контроль за соблюдением мер, обеспечивающих сохранность коммерческой тайны в отношении секрета производства (ноу-хау) СПбПУ, возлагается на директора Центра интеллектуальной собственности и трансфера технологий.

8.18. Процедура обеспечения правовой охраны результатов интеллектуальной деятельности в научно-технической сфере, отнесенных к секретам производства и подлежащих охране в режиме коммерческой тайны регламентируется Положением о порядке введения режима коммерческой тайны в отношении секрета производства ФГАОУ ВО «СПбПУ» (приказ ректора от 28.12.2023 № 3269 «Об утверждении Положения о порядке введения режима коммерческой тайны в отношении секрета производства»).

9. Порядок обращения со сведениями, составляющими служебную тайну

9.1. Порядок обращения в СПбПУ со сведениями, составляющими служебную тайну, регламентируется Инструкцией по обращению со служебной информацией ограниченного распространения в ФГАОУ ВО «СПбПУ» (Приложение №2 к настоящему Положению).

10. Порядок обработки конфиденциальной информации на средствах и системах информатизации

10.1. В настоящем разделе приведены требования, определяющие порядок обработки конфиденциальной информации на средствах и системах информатизации СПбПУ, условия и порядок подключения пользователей, работающих с конфиденциальной информацией в электронном виде, к сетям общего пользования, а также рекомендации по обеспечению безопасности конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, режим защиты которой определяет собственник этих ресурсов, в соответствии с СТР-К (п. 2.3.) и Руководящим документом Гостехкомиссии России от 25.07.1997 «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

10.2. Защита конфиденциальной информации при работе пользователей со средствами и системами информатизации направлена на устранение основных угроз безопасности информации:

- несанкционированного доступа к информации, хранящейся и обрабатываемой во внутренних локальных вычислительных сетях (серверах, рабочих станциях) или на автономных персональных электронно-вычислительных машинах (далее - ПЭВМ), как из сетей общего пользования, так и из внутренних локальных вычислительных сетей (далее - ЛВС);
- несанкционированного доступа к коммуникационному оборудованию (маршрутизатору, концентратору, мосту, мультиплексору, серверу), соединяющему внутренние ЛВС СПбПУ с сетями общего пользования;
- несанкционированного доступа к данным (сообщениям), передаваемым между внутренними ЛВС и сетями общего пользования, включая их модификацию, имитацию и уничтожение;
- влияния на программное обеспечение вредоносных компьютерных программ (далее - компьютерных вирусов) из сетей общего пользования, как посредством приема вредоносных файлов, так и посредством электронной почты (далее - E-mail);
- внедрения программных закладок с целью получения несанкционированного доступа к информации, а также дезорганизации работы внутренней ЛВС и ее взаимодействия с сетями общего пользования;
- несанкционированной передачи защищаемой конфиденциальной информации ЛВС в сети общего пользования;
- возможности перехвата информации внутренней ЛВС за счет побочных электромагнитных излучений и наводок от основных технических средств, обрабатывающих такую информацию.

10.3. Подключение к внутренним ЛВС, в которых обрабатывается конфиденциальная информация, разрешается только после установки на средствах вычислительной техники средств защиты информации от несанкционированного доступа, отвечающих требованиям настоящего Положения.

10.4. Подключение пользователей СПбПУ, работающих с конфиденциальной информацией в электронном виде, к сетям общего

пользования осуществляется администратором внутренней ЛВС по решению руководителя структурного подразделения с обоснованием, содержащим следующие сведения (обоснование может корректироваться по требованиям администратора внутренней ЛВС):

- наименование сети общего пользования, к которой осуществляется подключение;
- состав подключаемых технических средств;
- предполагаемые виды работ и используемые прикладные сервисы сети общего пользования (E-Mail, FTP, HTTP и т.п.) для средств вычислительной техники в целом и для каждого пользователя в частности;
- режим подключения средств вычислительной техники и пользователей к сети общего пользования (постоянный, в т.ч. круглосуточный, временный);
- состав общего и индивидуального телекоммуникационного программного обеспечения средств вычислительной техники для пользователей (операционные системы, клиентские прикладные программы для сети - браузеры и т.п.);
- число и перечень предполагаемых пользователей (диапазон используемых IP- адресов);
- меры и средства защиты информации от несанкционированного доступа, которые будут применяться на средствах вычислительной техники, организация-изготовитель, сведения о сертификации, установщик, конфигурация, правила работы с ними;
- перечень сведений конфиденциального характера, обрабатываемых (хранимых) на средствах вычислительной техники, подлежащих передаче и получаемых в результате подключения к сети общего пользования.

10.5. Порядок подключения и взаимодействия средств и систем информатизации, с помощью которых выполняется обработка конфиденциальной информации, требования по обеспечению безопасности информации:

10.5.1. В случае необходимости подключения к сетям общего пользования, это подключение должно осуществляться через средства разграничения доступа в виде межсетевых экранов. Не допускается подключение в обход межсетевых экранов. Межсетевые экраны должны быть сертифицированы по требованиям безопасности информации. Доступ к межсетевому экрану, к средствам его конфигурирования должен осуществляться только администратором с консоли. Средства удаленного управления межсетевым экраном должны быть исключены из конфигурации. С помощью межсетевых экранов должно обеспечиваться создание сеансов связи пользователей с внешними серверами сетей общего пользования и получение с этих серверов только ответов на запросы пользователей. Настройка межсетевого экрана должна обеспечивать отказ в обслуживании любых внешних запросов, которые могут направляться на защищаемые средства и системы информатизации СПбПУ. Устанавливаемые межсетевые экраны должны соответствовать классу защищаемого средства вычислительной

техники (автоматизированной системы) и отвечать требованиям руководящих документов.

10.5.2. При использовании почтового сервера и веб-сервера СПбПУ, последние не должны входить в состав используемой ЛВС и должны подключаться к сетям общего пользования по отдельному сетевому фрагменту (через маршрутизатор).

10.5.3. На технических средствах вычислительной техники должно находиться программное обеспечение только в той конфигурации, которая необходима для выполнения работ, заявленных в обосновании необходимости подключения средств вычислительной техники к сетям общего пользования.

10.6. Не допускается активизация не включенных в обоснование прикладных сервисов (протоколов) и не требующих привязки протоколов к портам.

10.7. Установку программного обеспечения, обеспечивающего функционирование средств вычислительной техники, выполняют уполномоченные специалисты под контролем администратора внутренней ЛВС. Пользователи средств вычислительной техники не имеют права производить самостоятельную установку и модификацию указанного программного обеспечения, однако должны обращаться к администратору для проведения его экспертизы на предмет улучшения характеристик, наличия компьютерных вирусов, замаскированных возможностей выполнения непредусмотренных действий. Вся ответственность за использование не прошедшего экспертизу и не рекомендованного к использованию программного обеспечения целиком ложится на пользователя средств вычислительной техники. При обнаружении фактов такого рода администратор обязан логически (а при необходимости - физически вместе с включающей подсетью) отключить средства вычислительной техники пользователя от всех информационных сетей и поставить об этом в известность соответствующих должностных лиц.

10.8. Системы защиты информации от несанкционированного доступа, устанавливаемые на автономные ПЭВМ, рабочие станции и серверы внутренних ЛВС СПбПУ при обработке на них конфиденциальной информации, должны осуществлять:

- идентификацию и аутентификацию пользователей при доступе к автономной ПЭВМ, рабочим станциям и серверам внутренней ЛВС по идентификатору и паролю;
- контроль доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС на основе дискреционного принципа;
- регистрацию доступа к ресурсам автономной ПЭВМ, рабочих станций и серверов внутренней ЛВС, включая попытки несанкционированного доступа;
- регистрацию фактов отправки и получения пользователем сообщений (файлов, писем, документов).

10.9. Система защиты информации от несанкционированного доступа должна запрещать запуск пользователями произвольных программ, не включенных в состав программного обеспечения ПЭВМ.

10.10. Модификация конфигурации программного обеспечения должна быть доступна только со стороны администратора, ответственного за эксплуатацию средств вычислительной техники.

10.11. Средства регистрации и регистрируемые данные должны быть недоступны для пользователя.

10.12. Система защиты информации от несанкционированного доступа должна быть целостной, т.е. защищенной от несанкционированной модификации и не содержащей путей обхода механизмов контроля.

10.13. Тестирование всех функций системы защиты информации от несанкционированного доступа с помощью специальных программных средств должно проводится не реже одного раза в год.

10.14. Технические средства вычислительной техники должны быть размещены либо в отдельном помещении (при автономной ПЭВМ, подключенной к сети общего пользования), либо в рабочих помещениях пользователей с принятием организационных и технических мер, исключающих несанкционированную работу в сети общего пользования. В этих помещениях должно быть исключено ведение конфиденциальных переговоров, либо технические средства должны быть защищены с точки зрения электроакустики. В нерабочее время помещение автономной ПЭВМ либо соответствующего сервера сдается под охрану в установленном порядке.

10.15. При создании рабочего места пользователя:

10.15.1. Межсетевой экран для связи с внешними сетями общего пользования, веб-серверы, почтовые серверы размещаются в отдельном защищаемом помещении, доступ в которое имеет ограниченный круг лиц (ответственные специалисты, администраторы).

10.15.2. Администратором сети осуществляются периодические проверки работоспособности межсетевых экранов с помощью сканеров, имитирующих внешние атаки на внутреннюю ЛВС. На используемый межсетевой экран не устанавливаются какие-либо другие прикладные сервисы (СУБД, E-mail, прикладные серверы и т.п.).

10.15.3. Для предоставления прикладных сервисов применяется принцип минимальной достаточности. Услуги доступа к сети общего пользования не предоставляются тем пользователям средств вычислительной техники, которым не требуются доступ. Пользователям, которым необходима только электронная почта, предоставляется доступ только к ней.

10.15.4. Используются операционные системы со встроенными функциями защиты информации от несанкционированного доступа, перечисленными в пункте 10.8, или сертифицированные системы защиты информации от несанкционированного доступа.

10.15.5. Используются имеющиеся в маршрутизаторах средства разграничения доступа (фильтрации), включающие контроль по списку доступа, аутентификацию пользователей, взаимную аутентификацию маршрутизаторов.

10.15.6. В целях контроля за правомерностью использования средств вычислительной техники и выявления нарушений требований по защите

информации осуществляется анализ принимаемой и передаваемой информации, в том числе на наличие компьютерных вирусов. Копии исходящей электронной почты и отсылаемых в сеть общего пользования файлов должны направляться в адрес защищенного архива для возможности последующего анализа со стороны администратора (специалистов по защите информации).

10.15.7. Приказом по СПбПУ назначаются лица (пользователи), допущенные к работам в сетях общего пользования с соответствующими полномочиями, лица, ответственные за эксплуатацию средства вычислительной техники, на котором осуществляется обработка конфиденциальной информации, и лица, ответственные за контроль выполнения мероприятий по обеспечению безопасности информации при работе пользователей в информационных системах (руководители подразделений и администраторы).

10.15.8. Вопросы обеспечения безопасности информации на рабочем месте должны быть отражены в инструкции, определяющей:

- порядок подключения и регистрации пользователей;
- порядок установки и конфигурирования общесистемного, прикладного коммуникационного программного обеспечения (серверов, маршрутизаторов, шлюзов, мостов, межсетевых экранов, браузеров), их новых версий;
- порядок применения средств защиты информации от несанкционированного доступа при взаимодействии с сетью общего пользования;
- порядок работы пользователей в сети общего пользования, в том числе с электронной почтой, порядок выбора и доступа к внутренним и внешним серверам (веб-серверам);
- порядок отправки данных через сеть общего пользования (при необходимости);
- обязанности и ответственность пользователей и администратора внутренней ЛВС по обеспечению безопасности информации при взаимодействии с сетью общего пользования;
- порядок контроля за выполнением мероприятий по обеспечению безопасности информации и работой пользователей.

10.16. К работе в качестве пользователей информационных систем допускаются лица, ознакомленные с требованиями по взаимодействию с другими пользователями и обеспечению при этом безопасности информации, допущенные к самостоятельной работе в установленном порядке.

10.17. Пользователи информационных систем обязаны:

- знать порядок регистрации и взаимодействия;
- знать инструкцию по обеспечению безопасности информации на рабочем месте;
- знать правила работы с установленными средствами защиты информации от несанкционированного доступа;
- уметь пользоваться средствами защиты ПЭВМ от компьютерных вирусов.

10.18. При работе в информационной сети категорически запрещается:

− подключать технические средства (серверы, рабочие станции), имеющие выход к другим техническим средствам (сетям), не определенным в обосновании подключения;

− изменять состав и конфигурацию программных и технических средств рабочего места без санкции администратора и аттестационной комиссии;

− производить необоснованную отправку данных;

− использовать на рабочих местах неучтенные носители информации без соответствующей санкции администратора.

10.19. Ведение учета пользователей информационных систем организуется администраторами, осуществляющими подключение.

10.20. Контроль за выполнением мероприятий по обеспечению безопасности информации на рабочих местах возлагается на руководителей соответствующих подразделений и администраторов, определенных приказом по СПбПУ, а также на начальника отдела защиты конфиденциальной информации.

10.21. Средства и системы информатизации, с помощью которых выполняется обработка конфиденциальной информации, должны быть аттестованы на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну.

10.22. Программа аттестационных испытаний средств и систем информатизации определяется аттестационной комиссией.

10.23. Необходимым условием аттестации является соответствие аттестуемых средств и систем информатизации действующим требованиям законодательства в области безопасности информации.

10.24. Порядок аттестации средств и систем информатизации регламентируется Инструкцией по аттестации объектов информатизации ФГАОУ ВО «СПбПУ» на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну (Приложение №3 к настоящему Положению).

11. Порядок проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.)

11.1. Для осуществления конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.) с передачей сведений, составляющих конфиденциальную информацию, применяются меры по организационной и технической защите речевой информации.

11.2. Защита речевой информации обеспечивается техническими средствами и организационными мерами ограничительного характера, регламентирующими порядок использования выделенных помещений на период проведения конфиденциальных мероприятий.

11.3. Требования настоящего раздела направлены на обеспечение защиты информации, обсуждаемой в выделенных помещениях, от утечки по техническим каналам (акустическому, виброакустическому,

электроакустическим преобразованиям, внедрению электронных устройств перехвата информации) и составлены в соответствии с требованиями и рекомендациями СТР-К.

11.4. Руководители структурных подразделений, деятельность которых связана со сведениями, составляющими конфиденциальную информацию, планируют, согласовывают с проректором по информационным технологиям и цифровой трансформации и начальником отдела защиты конфиденциальной информации мероприятия по аттестации помещений для проведения конфиденциальных мероприятий.

11.5. Запрещается проведение совещаний, обсуждений, конференций, переговоров и т.п. по конфиденциальным вопросам в неаттестованных помещениях СПбПУ.

11.6. Помещения, в которых проводятся конфиденциальные мероприятия, должны быть аттестованы на соответствие требованиям по безопасности информации.

11.7. Разрешается осуществлять работы с конфиденциальной информацией на объектах информатизации, аттестованных для работы со сведениями, составляющими государственную тайну.

11.8. Программа аттестационных испытаний защищаемых помещений определяется аттестационной комиссией.

11.9. Необходимым условием аттестации является соответствие защищаемых помещений требованиям законодательства по безопасности информации.

11.10. Порядок аттестации защищаемых помещений регламентируется Инструкцией по аттестации объектов информатизации ФГАОУ ВО «СПбПУ» на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну (Приложение №3 к настоящему Положению).

11.11. Руководители структурных подразделений и работники СПбПУ, за которыми закреплены аттестованные помещения, несут ответственность за выполнение установленных во время аттестации условий эксплуатации помещений и требований по безопасности информации.

11.12. В случае обнаружения факта несанкционированного проникновения в аттестованные помещения, производится расследование, организуемое руководителем структурного подразделения, с обязательным составлением акта.

11.13. В случае изменения условий эксплуатации аттестованного помещения и технологии защиты информации, ответственный за аттестованное помещение обязан известить об этом начальника отдела защиты конфиденциальной информации для принятия решения о необходимости проведения дополнительной проверки эффективности системы защиты информатизации в помещении.

12. Порядок планирования работ по защите конфиденциальной информации

12.1. Работа по защите конфиденциальной информации в СПбПУ проводится в соответствии с годовыми планами.

12.2. Годовой план работы по защите конфиденциальной информации разрабатывается начальником отдела защиты конфиденциальной информации, согласовывается с руководителем Управления информационной безопасности и утверждается проректором по информационным технологиям и цифровой трансформации.

12.3. План должен содержать мероприятия по защите информации, выполняемые как специалистами по защите информации, так и другими структурными подразделениями, которые в силу своих функциональных обязанностей занимаются вопросами защиты конфиденциальной информации. В план включаются следующие разделы:

12.3.1. Мероприятия по выполнению решений контролирующих органов (ФСТЭК России, ФСБ России и т.п.), приказов и распоряжений вышестоящей организации по защите конфиденциальной информации.

12.3.2. Мероприятия по защите конфиденциальной информации в структурных подразделениях СПбПУ:

- определение и уточнение угроз безопасности конфиденциальной информации, особенностей административной и управленческой деятельности, требующих защиты;
- обследование, категорирование и аттестация выделенных помещений, а также эксплуатируемых в них средств и систем информатизации, с помощью которых выполняется обработка конфиденциальной информации;
- анализ деятельности структурных подразделений с целью оценки реальной опасности утечки конфиденциальной информации, перехвата, несанкционированного доступа к информации, выявления и закрытия возможных каналов утечки охраняемых сведений;
- контроль соблюдения работниками СПбПУ требований по защите конфиденциальной информации;
- инструктаж работников, допущенных для работы с конфиденциальной информацией;
- установка технических средств защиты конфиденциальной информации.

12.3.3. Организационно-методическое обеспечение работ по защите конфиденциальной информации:

- разработка, корректировка и согласование организационно-методических документов, планов, отчетов;
- составление заявок на приобретение технических средств защиты конфиденциальной информации;
- обучение работников СПбПУ.

12.3.4. Контрольные мероприятия:

− оценка достаточности применяемых мер и средств защиты конфиденциальной информации;

− периодические проверки эффективности применяемых технических средств защиты конфиденциальной информации;

− участие в работе контролирующих органов.

13. Порядок контроля состояния защиты конфиденциальной информации

13.1. Контроль состояния защиты конфиденциальной информации осуществляется с целью своевременного выявления и предотвращения утечки конфиденциальной информации по техническим каналам, несанкционированного доступа к ней, преднамеренного программно-технического воздействия на информацию.

13.2. Постоянный контроль состояния защиты конфиденциальной информации в подразделениях СПбПУ осуществляют специалисты по защите информации, руководители структурных подразделений и администраторы по обеспечению безопасности информации.

13.3. Защита конфиденциальной информации считается эффективной, если принимаемые меры соответствуют установленным требованиям. Выявленные в результате контроля несоответствия мер установленным требованиям или нормам по защите конфиденциальной информации классифицируются как нарушения.

13.4. Периодический контроль деятельности по защите информации в подразделениях СПбПУ осуществляется специалистами отдела защиты конфиденциальной информации.

13.5. При обнаружении нарушений мер по защите конфиденциальной информации, руководители структурных подразделений СПбПУ обязаны принять меры по их устранению в сроки, согласованные с лицами, проводившими проверку.

13.6. По результатам проверки оформляется акт, в котором указывают:

− состав комиссии;

− сроки и цель проверки, краткая характеристика и оценка общего состояния работ по защите конфиденциальной информации, выявленные недостатки и их причины;

− выводы и рекомендации по результатам проверки.

13.7. Результаты проверки докладываются проректору по информационным технологиям и цифровой трансформации.

14. Взаимодействие с другими организациями в области защиты конфиденциальной информации

14.1. СПбПУ осуществляет взаимодействие по вопросам организации защиты конфиденциальной информации и контроля ее эффективности с

Управлением ФСТЭК России по Северо-Западному Федеральному округу и организациями, имеющими государственные лицензии и аккредитации в области защиты конфиденциальной информации.

14.2. Для обмена конфиденциальной информацией со сторонними организациями необходимо руководствоваться договорами и соглашениями, содержащими условия проведения работ или оказания услуг, цель и способы обмена конфиденциальной информацией, права и обязанности взаимодействующих сторон в области защиты конфиденциальной информации.

14.3. Передача конфиденциальной информации другим организациям возможна только при наличии в принимающих организациях условий, обеспечивающих безопасность конфиденциальной информации.

14.4. При возникновении необходимости проведения совместных организационно-технических мероприятий с другими организациями должны разрабатываться единые документы по защите конфиденциальной информации для всех этапов работ, утверждаемые руководителями взаимодействующих организаций.

15. Порядок принятия и внесения изменений

15.1. Настоящее Положение утверждается приказом ректора.

15.2. Основанием для внесения изменений могут быть изменения условий деятельности СПбПУ в целом, включая изменения учредительных документов, изменение законодательства, а также предложения работников СПбПУ.

15.3. Предложения по изменению или дополнению настоящего Положения направляются для рассмотрения проректору по информационным технологиям и цифровой трансформации. Проректор по информационным технологиям и цифровой трансформации принимает решение по результатам рассмотрения предложения, дает указание начальнику отдела защиты конфиденциальной информации подготовить проект изменений в настоящее Положение, которые принимаются и утверждаются приказом ректора.

Приложение № 1
к Положению об организации защиты
конфиденциальной информации
в ФГАОУ ВО «СПбПУ»

Перечень сведений, составляющих конфиденциальную информацию ФГАОУ ВО «СПбПУ»

Перечень сведений, составляющих конфиденциальную информацию ФГАОУ ВО «СПбПУ» (далее – Перечень конфиденциальной информации, СПбПУ) разработан в соответствии:

- с Федеральным законом от 29.07.2004 №98-ФЗ «О коммерческой тайне»;
- с Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»;
- с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;
- с Указом Президента Российской Федерации от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера»;
- с Инструкцией о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки Российской Федерации, утвержденной приказом Министерства образования и науки Российской Федерации от 30.12.2010 № 2233;
- с Уставом СПбПУ.

1. Персональные данные:

1.1. Фамилия, имя, отчество (в том числе прежние фамилия, имя или отчество в случае их изменения, когда, где и по какой причине изменяли).

1.2. Фотография.

1.3. Число, месяц, год рождения.

1.4. Место рождения.

1.5. Информация о гражданстве (в том числе прежние гражданства, иные гражданства).

1.6. Сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании).

1.7. Сведения о зачислении, переводе и отчислении обучающихся.

1.8. Сведения о профессиональной переподготовке и (или) повышении квалификации.

1.9. Сведения об ученой степени, ученом звании.

1.10. Информация о владении иностранными языками, степень владения.

1.11. Сведения из заключения медицинского учреждения о наличии (отсутствии) заболевания.

1.12. Сведения о прохождении службы (работы), в том числе: личный номер (при наличии), дата, основания поступления на службу (работу) и назначения на должность, дата, основания назначения, перевода, перемещения на иную должность, наименование замещаемых должностей с указанием структурных подразделений, размера денежного содержания, денежного довольствия, заработной платы, результатов аттестации на соответствие замещаемой должности, а также сведения о прежних местах службы (работы).

1.13. Информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору.

1.14. Сведения об участии в конференциях, фестивалях, конкурсах, соревнованиях и т.п., о достигнутых в их ходе результатах.

1.15. Информация о государственных наградах, иных наградах и знаках отличия (кем и когда награжден).

1.16. Информация об отпусках.

1.17. Сведения о доходах, расходах, об имуществе и обязательствах имущественного характера.

1.18. Сведения о социальных льготах, о назначении и получении стипендий, премий и других выплат.

1.19. Серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи.

1.20. Место жительства (адрес регистрации, фактического проживания) и адреса прежних мест жительства.

1.21. Номер личного или домашнего телефона.

1.22. Реквизиты страхового свидетельства обязательного пенсионного страхования.

1.23. Идентификационный номер налогоплательщика.

1.24. Реквизиты полиса обязательного медицинского страхования.

1.25. Семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших).

1.26. Информация, содержащаяся в свидетельствах о государственной регистрации актов гражданского состояния.

1.27. Сведения о воинском учете и информация, содержащаяся в документах воинского учета.

1.28. Персональные данные, содержащиеся в выписке из домовой книги, копиях финансового лицевого счета.

1.29. Сведения о пребывании за границей.

1.30. Информация о наличии (отсутствии) судимости.

1.31. Номер расчетного счета.

1.32. Номер банковской карты.

1.33. Иные персональные данные, необходимые для достижения целей их обработки.

1.34. Номер визы, миграционной карты, КПП въезда, дата пересечения границы Российской Федерации (для иностранных граждан).

1.35. Сроки пребывания на территории Российской Федерации и в СПбПУ (для иностранных граждан).

2. Информация, составляющая коммерческую тайну:

2.1. Сведения о коммерческих замыслах и планах (расширении или свертывании работ в целом и по отдельным направлениям).

2.2. Содержание и условия коммерческих контрактов, договоров, соглашений и платежей.

2.3. Сведения о целях, задачах, тактике и результатах переговоров с деловыми партнерами.

2.4. Сведения, составляющие секреты производства (ноу-хау).

2.5. Сведения, составляющие коммерческую тайну партнеров, переданные на доверительной основе.

2.6. Содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности.

2.7. Сведения об инвестициях.

2.8. Сведения, содержащие выводы и рекомендации по рыночной стратегии и тактике.

2.9. Сведения о фактическом состоянии расчетов по обязательствам.

2.10. Сведения об отдельных финансовых операциях СПбПУ и о доходах по этим операциям.

2.11. Сведения о внешнеэкономических, валютных и кредитных отношениях с конкретными иностранными и российскими предприятиями, фирмами и организациями.

2.12. Сведения о встречах и переговорах с деловыми партнерами СПбПУ.

2.13. Сведения об особых условиях отношений с иностранными научными и иными организациями.

2.14. Сведения о времени выхода на рынок, выбор посредника для ведения коммерческих переговоров и тактике их ведения.

2.15. Сведения о целях, задачах, программах, новейших по тематике и перспективных научно-технических работ и исследований.

2.16. Научно-техническая, технологическая, конструкторская и проектная документация.

2.17. Современные методы решения новых научных и научно-технических задач.

2.18. Новые высокоэффективные технические решения, не защищенные патентным правом, обеспечивающие значительное улучшение основных технико-экономических характеристик устройств и систем.

2.19. Современные методы проектирования и испытания современных и перспективных устройств и систем.

2.20. Информация о новых разработках программного и компьютерного обеспечения.
2.21. Экспериментальные и расчетные результаты, получение которых связано с большими финансовыми, материальными или временными издержками.
2.22. Информация о рентабельности научно-исследовательских работ СПбПУ.
2.23. Информация о себестоимости и контрактных ценах научных разработок, товаров, услуг, условиях кредитования и платежа.
2.24. Информация о конъюнктуре рынка научно-технических исследований и разработок, сведения о научно-исследовательских работах, выполняемых СПбПУ по государственным и муниципальным контрактам, хозяйственным договорам, инновационным проектам и т.д.
2.25. Информация об экспертизе научных трудов (публикаций).
2.26. Сведения о сущности изобретения, полезной модели, промышленного образца до официальной их регистрации.
2.27. Современные и эффективные технологии и методики обучения.
2.28. Результаты дипломных проектов, учебно-исследовательских работ студентов и аспирантов, имеющие практическую ценность.
2.29. Содержание современных учебных планов и программ, учебно-методических разработок по новым дисциплинам до их официального опубликования.
2.30. Сведения о конъюнктуре рынка подготовки специалистов.
2.31. Сведения о контрактах с иностранными гражданами.
2.32. Иные сведения, режим коммерческой тайны на которые распространяется по приказу ректора.

3. Информация, составляющая служебную тайну:
3.1. Сведения о перспективных методах управления СПбПУ.
3.2. Сведения о ведении и содержании переговоров, целях и содержании совещаний органов управления СПбПУ.
3.3. Сведения, содержащиеся в документах по организации воинского учета и мобилизационной работы, не относящиеся к государственной тайне.
3.4. План гражданской обороны СПбПУ.
3.5. Схемы размещения инфраструктуры жизнеобеспечения (энергоснабжения, водоснабжения, канализации, теплоснабжения, телефонной связи и др.).
3.6. Содержание переписки, телефонных переговоров, почтовых отправлений, телеграфных, электронных и иных сообщений.
3.7. Сведения об организации и состоянии системы безопасности жизнедеятельности, в том числе системы защиты информации.
3.8. Сведения об организации и состоянии охраны (пропускного и внутриобъектового режима).
3.9. Размещение защищаемых помещений (в которых хранится, циркулирует и обрабатывается конфиденциальная и другая ценная информация со средствами ее хранения, обработки и передачи), организация доступа в них.

3.10. Организация, схемы размещения, возможности и состояние системы охраны техническими средствами, в том числе системы видеонаблюдения, номера электронных ключей.

3.11. Организация, возможности и состояние оперативной связи обеспечения и безопасности жизнедеятельности.

3.12. Организация взаимодействия с правоохранительными и другими государственными органами при проведении совместных мероприятий.

3.13. Сведения, составляющие материалы служебных расследований, проверок, дознания, следствия, судопроизводства.

3.14. Проектная, техническая, эксплуатационная документация на автоматизированные системы, вычислительные сети, средства связи, в которых обрабатывается и циркулирует конфиденциальная информация (далее – АС, ВС, СС КИ).

3.15. Схемы размещения технических средств обработки конфиденциальной информации, коммуникационных линий.

3.16. Сведения о специфических и уникальных программных продуктах.

3.17. Ключи шифрования и электронно-цифровые подписи средств криптографической защиты информации, места и порядок их хранения и выдачи.

3.18. Порядок использования, возможности и состояние систем (средств) криптографической и технической защиты информации, документация на них.

3.19. Организация и состояние систем администрирования, управления доступом АС, ВС, СС КИ.

3.20. Порядок и места размещения информационных ресурсов, содержащих конфиденциальную информацию в СПбПУ.

3.21. Организация и состояние системы парольной защиты (значение, порядок генерации, использования, смены и прекращения действия кодов и паролей) в АС, ВС, СС КИ.

3.22. Организация резервирования конфиденциальной информации, места хранения резервных копий конфиденциальной, ценной и другой важной информации.

3.23. Программное обеспечение базового уровня оборудования средств связи.

3.24. База данных абонентских номеров телефонной связи.

3.25. Сводный перечень работ СПбПУ на перспективу, на год (квартал).

4. Сведения, содержащиеся в документах государственных органов, органов местного самоуправления, других организаций и учреждений с грифом «Для служебного пользования», «Коммерческая тайна», «Конфиденциальная информация».

Приложение № 2
к Положению об организации защиты
конфиденциальной информации
в ФГАОУ ВО «СПбПУ»

Инструкция по обращению со служебной информацией ограниченного распространения в ФГАОУ ВО «СПбПУ»

1. Общие положения

1.1. Инструкция по обращению со служебной информацией ограниченного распространения в ФГАОУ ВО «СПбПУ» (далее соответственно - Инструкция, СПбПУ) определяет порядок обращения со служебными документами (договорами, письмами, протоколами, актами и др.) и другими материальными носителями информации (машинные носители информации и др.), содержащими служебную информацию ограниченного доступа (распространения), с учетом требований:

- Федерального закона от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, утвержденного постановлением Правительства Российской Федерации от 3 ноября 1994 г. №1233;
- Инструкции о порядке обращения со служебной информацией ограниченного распространения в Министерстве образования и науки Российской Федерации (утв. Приказом Министерства образования и науки Российской Федерации от 30 декабря 2010 г. №2233);
- Приказа Министерства науки и высшего образования Российской Федерации от 22 октября 2018 г. №51н «Об упорядочении обращения со служебной информацией ограниченного распространения в Министерстве науки и высшего образования Российской Федерации и его территориальных органах» (вместе с «Порядком передачи служебной информации ограниченного распространения другим органам и организациям», «Порядком снятия пометки «Для служебного пользования» с носителей информации ограниченного распространения»).

1.2. Настоящая Инструкция не распространяется на порядок обращения с документами и другими материальными носителями информации, содержащими сведения, составляющие государственную тайну.

1.3. К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности СПбПУ, ограничение на распространение которой диктуется служебной необходимостью.

1.4. На документах (в необходимых случаях - и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования».

1.5. На машиночитаемых носителях, содержащих служебную информацию ограниченного распространения, пометка о конфиденциальности служебной информации может иметь вид «ДСП».

1.6. Относить служебную информацию к разряду ограниченного распространения, в соответствии с утвержденным Перечнем сведений, составляющих конфиденциальную информацию ФГАОУ ВО «СПбПУ», уполномочены должностные лица, указанные в пункте 2.1 настоящей Инструкции, и ответственные лица, назначенные приказом проректора по информационным технологиям и цифровой трансформации.

1.7. Снятие отметки «Для служебного пользования» с документов производится исполнителем, его непосредственным руководителем или начальником отдела защиты конфиденциальной информации в случаях:

- необоснованного отнесения к категории ограниченного распространения;
- изменений объективных обстоятельств, вследствие которых дальнейшая защита служебной информации ограниченного распространения нецелесообразна.

1.8. Исполнители, принявшие решение об отнесении служебной информации к разряду ограниченного распространения, несут персональную ответственность за обоснованность принятого решения, за соблюдение ограничений, предусмотренных пунктом 2.4 настоящей Инструкции.

1.9. Проректор по информационным технологиям и цифровой трансформации, начальник Управления информационной безопасности, начальник Управления делами, начальник спецотдела и начальник отдела защиты конфиденциальной информации вправе вносить предложения ответственным лицам, уполномоченным относить служебную информацию к разряду ограниченного распространения (пункт 1.6 настоящей Инструкции), о внесении или снятии пометки «Для служебного пользования» по разрабатываемым или уже действующим документам.

1.10. Ответственные лица, уполномоченные относить служебную информацию к разряду ограниченного распространения (пункт 1.6 настоящей Инструкции), устанавливают перечень лиц, организаций, которым направляется документ с пометкой «Для служебного пользования».

1.11. Служебная информация ограниченного распространения не подлежит разглашению (распространению) без санкции соответствующего ответственного лица, его непосредственного руководителя, ректора, проректора по направлению деятельности.

1.12. За разглашение служебной информации ограниченного распространения, а также за нарушение порядка обращения с документами, содержащими такую информацию, работники СПбПУ могут быть привлечены

к дисциплинарной или иной предусмотренной законодательством Российской Федерации ответственности.

1.13. Контроль за соблюдением установленных правил и порядка обращения со служебной информацией ограниченного распространения в СПбПУ возлагается на начальника отдела защиты конфиденциальной информации и руководителей структурных подразделений.

1.14. В случае исключения из структуры СПбПУ (прекращения деятельности) структурных подразделений, решение о дальнейшем использовании служебной информации ограниченного распространения, находящейся в подразделениях, прекративших деятельность, принимает комиссия, назначенная приказом по СПбПУ.

2. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения

2.1. Необходимость проставления отметки «Для служебного пользования» на документах и изданиях, содержащих служебную информацию ограниченного распространения, определяется ответственным лицом (исполнителем) и должностным лицом, подписывающим или утверждающим документ. Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы документа, на обложке и титульном листе издания, а также на первой странице сопроводительного письма к таким документам.

2.2. Учет (регистрацию) внутренних документов СПбПУ, содержащих информацию ограниченного распространения, осуществляет исполнитель, в соответствии с инструкцией по конфиденциальному делопроизводству в ФГАОУ ВО «СПбПУ».

2.3. Прием и учет (регистрацию) документов сторонних организаций, содержащих информацию ограниченного распространения, осуществляет Канцелярия СПбПУ по соответствующему сопроводительному письму.

2.4. Документы с пометкой «Для служебного пользования»:

2.4.1. Создаются на автоматизированном рабочем месте с закрытым доступом в информационные сети общего пользования. На обороте последнего листа каждого экземпляра документа исполнитель должен указать количество отпечатанных экземпляров, свою фамилию и дату печатания документа. Регистрируются все отпечатанные и подписанные документы вместе со всеми черновиками и вариантами. Черновики и варианты уничтожаются ответственными лицами с отражением факта уничтожения в акте.

2.4.2. Учитываются отдельно от других документов, не имеющих пометку «Для служебного пользования». При незначительном объеме таких документов разрешается вести их учет совместно с другими документами. При регистрации указанных документов к регистрационному индексу документа добавляется пометка «ДСП».

2.4.3. Передаются работникам структурных подразделений под расписку.

2.4.4. Пересылаются сторонним организациям фельдъегерской связью, заказными или ценными почтовыми отправлениями, а также могут быть переданы нарочным.

2.4.5. Размножаются (тиражируются) только с письменного указания должностного лица, уполномоченного относить служебную информацию к разряду ограниченного распространения, в соответствии с пунктом 1.6 настоящей Инструкции. Учет размноженных документов осуществляется поэкземплярно. Перед размножением на титульном листе оригинала документа проставляется отметка о размножении с указанием регистрационного номера по журналу учета размножения служебных документов. На обороте последнего листа оригинала размножаемого экземпляра документа исполнитель должен указать регистрационный номер по журналу учета размножения служебных документов, количество размноженных экземпляров, свою фамилию и дату размножения документа. Нумерация дополнительно размноженных экземпляров производится от последнего номера ранее учтенного экземпляра этого документа.

2.4.6. Хранятся в надежно закрываемых и опечатываемых шкафах (ящиках, хранилищах).

2.5. Запрещается сканирование - введение в систему электронного документооборота электронной версии документов с пометкой «Для служебного пользования».

2.6. Не допускается передача в устной форме сведений, содержащихся в документах с пометкой «Для служебного пользования», без разрешения должностного лица, уполномоченного относить служебную информацию к разряду ограниченного распространения, в соответствии с пунктом 1.6 настоящей Инструкции.

2.7. При необходимости направления документов с пометкой «Для служебного пользования» в несколько адресов, составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем документа и руководителем структурного подразделения, подготовившего документ.

2.8. Для передачи документов с пометкой «Для служебного пользования» используются конверты, изготовленные из плотной бумаги. На конверте указываются пометка «Для служебного пользования», адрес получателя, а под ним данные об отправителе корреспонденции и регистрационные номера вложенных в конверт документов.

2.9. При направлении нескольких экземпляров одного документа на конверте и в реестре после регистрационного номера документа в скобках указываются номера экземпляров.

2.10. Отправка документов с пометкой «Для служебного пользования» средствами факсимильной связи, электронной почты запрещена.

2.11. Исполненные документы с пометкой «Для служебного пользования» группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. При этом на обложке дела, в которое

помещены такие документы, также проставляется пометка «Для служебного пользования».

2.12. Уничтожение дел, документов с пометкой «Для служебного пользования», утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт. Не допускается неполное уничтожение дел и документов с пометкой «Для служебного пользования», позволяющее восстановить их содержание.

2.13. Передача документов и дел с пометкой «Для служебного пользования» от одного работника другому осуществляется с разрешения должностного лица (с резолюцией в сопроводительном письме или в графе «Примечание» журнала регистрации исходящих конфиденциальных документов подразделения), в соответствии с разделом 4 настоящего Положения и инструкцией по конфиденциальному делопроизводству в ФГАОУ ВО «СПбПУ».

2.14. При смене работника, ответственного за учет документов с пометкой «Для служебного пользования», составляется акт приема-сдачи этих документов, который утверждается проректором по направлению деятельности.

2.15. Проверка наличия документов, дел и изданий с пометкой «Для служебного пользования» проводится не реже одного раза в год комиссиями, назначаемыми приказами по СПбПУ. В состав указанных комиссий обязательно включаются работники, ответственные за учет и хранение этих документов.

2.16. О фактах утраты документов, дел и изданий, содержащих служебную информацию ограниченного распространения, либо разглашения этой информации, ставится в известность начальник отдела защиты конфиденциальной информации или проректор по информационным технологиям и цифровой трансформации и назначается комиссия для служебного расследования обстоятельств утраты или разглашения. Результаты служебного расследования докладываются соответствующим проректорам или ректору СПбПУ в зависимости от выявленных в ходе расследования обстоятельств.

2.17. При снятии пометки «Для служебного пользования» на документах, делах или изданиях, а также в учетных формах делаются соответствующие отметки и информируются все адресаты, которым эти документы (издания) направлялись.

Приложение № 3
к Положению об организации защиты
конфиденциальной информации
в ФГАОУ ВО «СПбПУ»

Инструкция по аттестации объектов информатизации ФГАОУ ВО «СПбПУ» на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну

1. Инструкция по аттестации объектов информатизации ФГАОУ ВО «СПбПУ» на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну (далее соответственно - Инструкция, СПбПУ) разработана в соответствии с Положением по аттестации объектов информатизации по требованиям безопасности информации (утв. Гостехкомиссией России 25.11.1994), Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (утв. приказом Гостехкомиссии России от 30.08.2002 №282, далее - СТР-К) и Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (далее - приказ ФСТЭК № 17).

2. Настоящая Инструкция определяет порядок аттестации объектов информатизации, предназначенных для обработки конфиденциальной информации и проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

3. К аттестуемым объектам информатизации СПбПУ относятся:

− средства и системы информатизации, включая автоматизированные (информационные) системы различного уровня и назначения, системы связи, приема, обработки и передачи данных, системы отображения и размножения информации, с помощью которых выполняется обработка конфиденциальной информации;

− помещения, в которых выполняется обработка конфиденциальной информации и проводятся конфиденциальные мероприятия.

4. Аттестацией объектов информатизации является комплекс организационно-технических мероприятий, в результате которых посредством специального документа (далее - Аттестат соответствия) подтверждается соответствие объектов информатизации требованиям стандартов или иных нормативно-технических документов по безопасности информации.

5. Наличие у объекта информатизации действующего Аттестата соответствия, с установленным уровнем защищенности, дает право на обработку определенных категорий данных в указанный период времени.

6. Аттестация объектов информатизации СПбПУ проводится комиссией, созданной приказом ректора или специализированной

организацией, имеющей подтверждение аккредитации и лицензию ФСТЭК России.

7. Аттестацию объектов информатизации на соответствие требованиям безопасности конфиденциальной информации могут осуществлять организации-лицензиаты ФСТЭК России, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Постановлением Правительства Российской Федерации от 03.02.2012 №79 «О лицензировании деятельности по технической защите конфиденциальной информации». В перечне работ и услуг лицензии организации-лицензиата должно быть указано – аттестационные испытания и аттестация на соответствие требованиям по защите информации и перечислены типы объектов информатизации, которые организация может аттестовать.

8. Аттестация автоматизированной системы СПбПУ комиссией, созданной приказом ректора, проводится при условии, что система создана за счет средств вуза, а также обрабатываемая и защищаемая информация относится строго к автоматизированной системе СПбПУ.

9. Не допускается проведение аттестационных испытаний информационных систем должностными лицами, осуществляющими проектирование и (или) внедрение системы защиты информации аттестуемой информационной системы, в соответствии с пунктом 17 приказа ФСТЭК №17.

10. В состав аттестационной комиссии включаются квалифицированные специалисты, имеющие образование в области защиты информации, необходимые навыки для аттестации конкретного объекта информатизации, а также имеющие практический опыт проведения аналогичных работ и не участвующие непосредственно в обеспечении работы аттестуемого объекта информатизации.

11. Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью подтверждения эффективности комплекса используемых на конкретном объекте информатизации мер и средств защиты конфиденциальной информации.

12. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

13. Аттестация проводится в установленном настоящей Инструкцией порядке, в соответствии со схемой, выбираемой на этапе подготовки к аттестации из следующего основного перечня работ:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;

− проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;

− проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;

− проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;

− анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

14. Руководитель структурного подразделения или работник СПбПУ, в ответственности которого находится аттестуемый объект информатизации:

− сообщает служебной запиской о необходимости проведения аттестации проректору по информационным технологиям и цифровой трансформации;

− проводит подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;

− оформляет заявку на проведение аттестации;

− в необходимых случаях организовывает подписание договора со специализированной организацией для проведения аттестации объекта информатизации;

− предоставляет необходимые документы и условия для проведения аттестации;

− осуществляет эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в Аттестате соответствия;

− извещает орган по аттестации, выдавший Аттестат соответствия, о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в Аттестате соответствия);

− предоставляет необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего аттестацию.

15. Начальник отдела защиты конфиденциальной информации:

− организует проведение аттестации объектов информатизации на основании служебных записок, согласованных проректором по информационным технологиям и цифровой трансформации;

− в случае выявления неаттестованных объектов информирует руководителей структурных подразделений и работников СПбПУ, в ответственности которых находятся объекты информатизации, о необходимости проведения аттестации;

− осуществляет контроль и периодические проверки функционирования аттестованных объектов информатизации.

16. Порядок проведения аттестации на этапе аттестационных испытаний объекта информатизации:

− осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте, разработанной документации и ее соответствия требованиям нормативной документации по защите информации;

− определяется правильность категорирования объекта информатизации и классификации автоматизированных систем (при аттестации автоматизированных систем), выбора и применения сертифицированных и несертифицированных средств и систем защиты информации;

− проводятся испытания несертифицированных средств и систем защиты информации на аттестуемом объекте или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации;

− проверяется уровень подготовки кадров и распределение ответственности персонала за обеспечение выполнения требований по безопасности информации;

− проводятся комплексные аттестационные испытания объекта информатизации в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки защищаемой информации;

− оформляются протоколы испытаний и заключение по результатам аттестации с конкретными рекомендациями по устранению допущенных нарушений, приведению системы защиты объекта информатизации в соответствие с установленными требованиями и совершенствованию этой системы, а также рекомендациями по контролю за функционированием объекта информатизации.

17. Требования к нормативным и методическим документам, применяемым для аттестации объектов информатизации:

− состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется аттестационной комиссией в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту;

− объекты информатизации, вне зависимости от используемых отечественных или зарубежных технических и программных средств, аттестуются на соответствие требованиям государственных стандартов или иных нормативных документов по безопасности информации, утвержденных ФСТЭК России (Гостехкомиссией России);

− в нормативной и методической документации должно содержаться указание о возможности использования документа для аттестации определенных типов объектов информатизации по требованиям безопасности информации или направлений защиты информации.

18. Порядок оформления документов по результатам аттестации:

− оформляется заключение с краткой оценкой соответствия объекта информатизации требованиям по безопасности информации, выводом о возможности выдачи Аттестата соответствия и необходимыми рекомендациями;

− заключение подписывается членами аттестационной комиссии и доводится до сведения заявителя;

− к заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод;

− протоколы испытаний подписываются экспертами - членами аттестационной комиссии, проводившими испытания;

− заключение и протоколы испытаний подлежат утверждению руководителем организации, проводившей аттестацию;

− все документы по аттестации оформляются на русском языке по форме, приведенной в СТР-К.

19. Перечень форм документов, приведенных в СТР-К и оформляемых в результате аттестации:

− акт классификации автоматизированной системы обработки информации;

− аттестат соответствия автоматизированной системы требованиям по безопасности информации;

− аттестат соответствия защищаемого помещения требованиям по безопасности информации;

− форма технического паспорта на защищаемое помещение;

− форма технического паспорта на автоматизированную систему.

20. Порядок оформления, регистрации и получения Аттестата соответствия:

− Аттестат соответствия на объект информатизации, отвечающий требованиям по безопасности информации, выдается по форме, приведенной в приложении №2 СТР-К;

− Аттестат соответствия оформляется и выдается заявителю после утверждения заключения по результатам аттестации;

− Аттестат соответствия выдается заявителю на период, в течение которого обеспечивается неизменность условий функционирования объекта информатизации и технологии обработки защищаемой информации, могущих повлиять на характеристики, определяющие безопасность информации (состав и структура технических средств, условия размещения, используемое программное обеспечение, режимы обработки информации, средства и меры защиты), но не более чем на 3 года;

− при несоответствии аттестуемого объектов на соответствие требованиям по защите информации ограниченного доступа, не составляющей государственную тайну, и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки принимается решение об отказе в выдаче Аттестата соответствия, при этом может быть предложен срок повторной аттестации при условии устранения недостатков;

− при наличии замечаний непринципиального характера Аттестат соответствия может быть выдан после проверки устранения этих замечаний.

21. Руководитель структурного подразделения или работник СПбПУ, в ответственности которого находится аттестованный объект информатизации, несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по защите информации ограниченного доступа, не составляющей государственную тайну.

22. В случае изменения условий и технологии обработки защищаемой информации ответственный за аттестованный объект обязан известить об этом начальника отдела защиты конфиденциальной информации для принятия решения о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

Приложение № 4
к Положению об организации защиты
конфиденциальной информации
в ФГАОУ ВО «СПбПУ»

Инструкция о порядке передачи информации, составляющей коммерческую тайну, и иной конфиденциальной информации органам государственной власти, иным государственным органам, органам местного самоуправления и контрагентам

Содержание:

Приложения:

1. Форма сопроводительного письма о предоставлении конфиденциальной информации.
2. Форма расписки об ознакомлении с конфиденциальной информацией.
3. Форма соглашения о конфиденциальности.

1. Общие положения

1.1. Настоящая Инструкция устанавливает в СПбПУ единый порядок передачи информации, составляющей коммерческую тайну, и иной конфиденциальной информации органам государственной власти, иным государственным органам или органам местного самоуправления (далее - органы государственной власти), контрагентам и является обязательной для исполнения всеми работниками СПбПУ.

1.2. Под передачей конфиденциальной информации органам государственной власти и контрагентам понимается доведение до их уполномоченных представителей каким-либо способом (передача, пересылка, ознакомление, осуществление доступа) указанной информации.

1.3. К конфиденциальной относится информация, подпадающая под действие Положения и изложенная в Перечне конфиденциальной информации.

1.4. СПбПУ является обладателем информации, включенной в состав информационных ресурсов и находящейся в распоряжении структурных подразделений, а также предоставленной в распоряжение его дочерних и зависимых обществ в установленном порядке.

1.5. Передача информации, составляющей коммерческую тайну, или иной конфиденциальной информации органам государственной власти и

контрагентам осуществляется на основании решения ректора и (или) проректора по направлениям деятельности.

1.6. До принятия решения о передаче конфиденциальной информации органам государственной власти и контрагентам, работники структурных подразделений СПбПУ информируют проректоров по направлениям деятельности о конфиденциальной информации, подлежащей передаче.

1.7. На документах или других материальных носителях информации, содержащих конфиденциальную информацию, должны быть проставлены грифы конфиденциальности в соответствии с требованиями Положения.

1.8. Конфиденциальная информация представляется по мотивированному требованию органа государственной власти на безвозмездной основе. Мотивированное требование должно быть подписано уполномоченным должностным лицом органа государственной власти, содержать указание цели и правового основания затребования конфиденциальной информации, срок представления этой информации, если иное не установлено федеральными законами.

1.9. Фактическая передача (пересылка) конфиденциальных документов органам государственной власти и контрагентам должна осуществляться в соответствии с инструкцией по конфиденциальному делопроизводству в ФГАОУ ВО «СПбПУ».

1.10. Передача конфиденциальной информации по незащищенным каналам связи (с использованием факсимильной связи, сетей Интернет и т.п.), без принятия достаточных мер по защите информации запрещается.

1.11. Руководители структурных подразделений, а также исполнители, осуществляющие подготовку и передачу информации органам государственной власти и контрагентам, несут персональную ответственность за нарушение или ненадлежащее исполнение настоящей Инструкции в соответствии с законодательством Российской Федерации и нормативными актами и документами по защите информации.

2. Передача конфиденциальной информации органам государственной власти

2.1. Документированная информация, в случаях прямо установленных законодательством, подлежащая передаче органам государственной власти в обязательном порядке и подпадающая под действие Перечня конфиденциальной информации, представляется структурными подразделениями этим органам по утвержденным ими формам и в установленные сроки без принятия решения должностными лицами, указанными в пункте 1.5.

2.2. Информация, составляющая коммерческую тайну и иная конфиденциальная информация, в обязательном порядке предоставляется судам, органам прокуратуры, органам предварительного следствия, органам дознания по делам, находящимся в их производстве, по их запросу в порядке и

на основаниях, которые предусмотрены законодательством Российской Федерации.

2.3. В случае, если орган государственной власти, в соответствии с законодательством Российской Федерации, обладает полномочиями для получения конфиденциальной информации, которая не подлежит представлению в обязательном порядке, то передача данной информации должна осуществляться после принятия решения должностными лицами, указанными в пункте 1.5, исключительно по письменным мотивированным требованиям (запросам), оформленным на официальных бланках и за подписью уполномоченных должностных лиц таких органов, с указанием цели и правового основания затребования информации и срока ее предоставления. При этом объем передаваемой конфиденциальной информации не должен превышать объема, который данный орган государственной власти уполномочен получать.

2.4. Руководители структурных подразделений, в ведении которых находится конфиденциальная информация, подлежащая в соответствии с поступившим требованием (запросом) предоставлению органам государственной власти, обязаны:

- проверить основания требований (запросов) на получение соответствующей информации;
- представить должностным лицам, указанным в пункте 1.5, справку-обоснование, согласованную в случае необходимости с отделом защиты конфиденциальной информации и Административно-правовым департаментом, для принятия решения о передаче информации.

2.5. При предоставлении органам государственной власти по их мотивированным запросам (требованиям) информации, составляющей коммерческую тайну СПбПУ, дочерних обществ и организаций, в сопроводительном письме должно быть указано, что в отношении передаваемой информации необходимо установить режим конфиденциальности (Приложение №1). На документах, содержащих такую информацию, должен быть проставлен гриф «Коммерческая тайна» с указанием ее обладателя.

2.6. Допуск к конфиденциальной информации уполномоченных должностных лиц органов государственной власти, прибывающих на законном основании в подразделения СПбПУ для проведения проверок, ревизий либо иных мероприятий, осуществляемых в рамках полномочий данных государственных органов, должен осуществляться на основании соответствующих предписаний, подписанных руководителями или уполномоченными лицами данных органов государственной власти, по решению ректора или проректоров по направлениям деятельности и по согласованию (при необходимости) с отделом защиты конфиденциальной информации и Административно-правовым департаментом.

2.7. При ознакомлении уполномоченных должностных лиц органов государственной власти с конфиденциальной информацией в период проведения ими проверок, ревизий либо иных мероприятий, осуществляемых в рамках полномочий данных органов государственной власти, они должны быть

предупреждены под роспись в Расписке, составленной по типовой форме (Приложение №2) о том, что предоставляемые им документы и материалы являются конфиденциальными.

3. Передача конфиденциальной информации контрагентам

3.1. Передача конфиденциальной информации контрагентам осуществляется на основании Соглашения о конфиденциальности, содержащего обязательства стороны, получающей конфиденциальную информацию, по защите и неразглашению третьим лицам передаваемой конфиденциальной информации. Типовая форма Соглашения о конфиденциальности приведена в Приложении №3. Допускаются отступления от типовой формы Соглашения о конфиденциальности, в том числе изменение названия документа, если это не повлияет на юридическую значимость документа и существенные обязательства сторон.

3.2. Соглашения о конфиденциальности подготавливаются исполнителями в структурных подразделениях СПбПУ, заинтересованных в передаче конфиденциальной информации (далее – Исполнитель) или ответственными лицами, назначенными соответствующими приказами.

3.3. При подготовке Соглашения о конфиденциальности с контрагентом, Исполнитель запрашивает у контрагента внутренние нормативные документы, регламентирующие вопросы защиты конфиденциальной информации. На основе анализа принимаемых контрагентом мер по охране конфиденциальной информации Исполнителем вносятся необходимые корректировки в проект Соглашения о конфиденциальности и принимается решение по дальнейшему взаимодействию с данным контрагентом. Проект Соглашения о конфиденциальности согласовывается с отделом защиты конфиденциальной информации и Управлением правового обеспечения.

3.4. Подготовленный и надлежащим образом оформленный проект Соглашения о конфиденциальности до представления его на подпись руководству подлежит согласованию в следующей последовательности:

- начальник (или лицо его замещающее) структурного подразделения Исполнителя;
- начальник (или лицо его замещающее) отдела защиты конфиденциальной информации;
- начальник (или лицо его замещающее) Управления правового обеспечения.

3.5. Руководители структурных подразделений, заинтересованных в передаче контрагентам конфиденциальной информации, в целях принятия лицами, указанными в пункте 1.5 обоснованного решения, представляют им экспертное заключение о возможности и экономической целесообразности такой передачи (справку-обоснование) и проект решения (либо проект сопроводительного письма к передаваемым материалам) по данному вопросу.

3.6. На основании решения, принятого в соответствии с процедурами, предусмотренными Соглашением о конфиденциальности, действующими

нормативными актами и документами по защите конфиденциальной информации договаривающихся сторон, осуществляется фактическая передача информации в соответствии с требованиями пункта 1.8 настоящей Инструкции.

Приложение №1
к Инструкции о порядке передачи информации,
составляющей коммерческую тайну,
и иной конфиденциальной информации
органам государственной власти и контрагентам

Форма сопроводительного письма о предоставлении конфиденциальной информации

(Оформляется на бланке ФГАОУ ВО «СПбПУ»)

Коммерческая тайна
ФГАОУ ВО «СПбПУ»
195251, г. Санкт-Петербург, вн.тер.г.
муниципальный округ Академическое,
Политехническая ул., д. 29, литера Б
Экз. №_____

Начальнику _____
по городу Санкт-Петербургу
и Ленинградской области
Иванову И.И.
191123, г. Санкт-Петербург,
ул. Ленинградская, д. 1.

_____ № _____
на №_____от _____20___г.

Сопроводительное письмо

В соответствии с запросом *(требованием)*_____направляем Вам необходимые материалы.

В связи с тем, что передаваемая информация составляет коммерческую тайну ФГАОУ ВО «СПбПУ» *(дочернего общества, организации)*, прошу установить в отношении нее режим конфиденциальности.

Приложение: *(наименование документа)*, коммерческая тайна, уч. №___, экз. №___, на ____л.

(если приложение не остается у исполнителя, после количества листов указываются слова «только адресату»).

(должность) (личная подпись) (инициалы, фамилия)

Приложение №2
к Инструкции о порядке передачи информации,
составляющей коммерческую тайну,
и иной конфиденциальной информации
органам государственной власти и контрагентам

Форма

Расписка об ознакомлении с конфиденциальной информацией

Я, _____,
(должность, фамилия, имя, отчество полностью)

с целью _____,
(комиссия, проверка и т.п.)

на основании _____,
(дата и номер предписания, подписанного руководителем или уполномоченным лицом органа государственной власти)

в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО «СПбПУ», адрес: 195251, г. Санкт-Петербург, вн.тер.г. муниципальный округ Академическое, ул Политехническая, д. 29, литера Б, ИНН 7804040077, ОГРН 1027802505279) был ознакомлен со следующими конфиденциальной информацией:

_____,
(коммерческая тайна, персональные данные, субъекты персональных данных и т.п.)

а также предупрежден о возможности наступления ответственности, предусмотренной законодательством Российской Федерации за неправомерное разглашение вышеуказанных персональных данных.

"___"_____ _____ г.

_____/_____
подпись *(фамилия, имя, отчество полностью)*

Приложение №3
к Инструкции о порядке передачи информации,
составляющей коммерческую тайну,
и иной конфиденциальной информации
органам государственной власти и контрагентам

Форма

СОГЛАШЕНИЕ
О КОНФИДЕНЦИАЛЬНОСТИ

г. Санкт-Петербург «___» _____ 20__ г.

_____, в лице _____, действующего на основании _____, и _____, в лице _____, действующего на основании _____, по отдельности именуемые **«Сторона»**, а вместе именуемые далее **«Стороны»** или в зависимости от отношения к передаваемой информации, как **«Передающая сторона»** или **«Принимающая сторона»**, с учетом того, что Стороны намереваются обмениваться конфиденциальной информацией, предметами, документацией и носителями данных, а также желают избежать несанкционированного использования такого рода информации, предметов, документации и носителей данных, заключили настоящее Соглашение о конфиденциальности (далее – «Соглашение»), вступающее в силу с момента подписания его обеими Сторонами, о нижеследующем:

1. Предмет Соглашения

1.1. В целях охраны конфиденциальной информации Сторон, а также в целях предупреждения недобросовестной конкуренции и нанесения Сторонам убытков, Стороны заключили настоящее Соглашение в рамках _____.

1.2. В соответствии с условиями Соглашения Стороны принимают на себя взаимные обязательства по неразглашению и защите конфиденциальной информации, получаемой Сторонами друг от друга.

2. Термины, употребляемые в Соглашении:

Для целей Соглашения Стороны признают однозначное толкование приведенных ниже терминов:

2.1. Конфиденциальная информация – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной

деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладатель таких сведений принимает разумные меры для соблюдения их конфиденциальности, в том числе путем введения режима коммерческой тайны.

2.2. Обладатель конфиденциальной информации – Передающая сторона, самостоятельно создавшая информацию либо получившая ее на законном основании, которая реализует право разрешать или ограничивать доступ к имеющейся в ее распоряжении информации.

2.3. Передающая сторона – Сторона, являющаяся обладателем конфиденциальной информации на праве собственности или ином законном основании и передающая такую информацию Принимающей стороне Соглашения.

2.4. Принимающая сторона – Сторона, получающая конфиденциальную информацию в пользование в рамках Соглашения.

2.5. Третьи лица – юридические лица, не являющиеся Сторонами Соглашения, а также физические лица, являющиеся работниками Сторон, но не привлеченные к исполнению обязательств по гражданско-правовому договору, соответствующему Соглашению.

2.6. Передача конфиденциальной информации – передача конфиденциальной информации, зафиксированной на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

2.7. Контрагент – сторона гражданско-правового договора, которой обладатель конфиденциальной информации, передал эту информацию.

2.8. Предоставление конфиденциальной информации – передача конфиденциальной информации, зафиксированной на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

2.9. Разглашение конфиденциальной информации – действие или бездействие, в результате которых конфиденциальной информация, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

2.10. Раскрытие информации – ознакомление определенных лиц, согласованных Сторонами, с конфиденциальной информацией при условии сохранения конфиденциальности этой информации.

2.11. Уничтожение информации – действия, в результате которых носители информации претерпевают такие изменения, что однозначное воспроизведение записанной на них информации становится невозможным.

3. Общие положения

3.1. Конфиденциальная информация, передаваемая в рамках настоящего Соглашения, должна быть специально помечена как конфиденциальная, до момента ее передачи.

3.2. Конфиденциальной информацией, в рамках настоящего соглашения, не является информация, которая:

– была или стала общеизвестной из источника, отличного от Принимающей стороны;

– была на законных основаниях известна Принимающей стороне до ее передачи от Передающей стороны;

– становится известной Принимающей стороне на не конфиденциальной основе из источника, не являющеюся Стороной настоящего Соглашения и без нарушения настоящего Соглашения;

– не может быть отнесена к конфиденциальной информации в соответствии с действующим законодательством Российской Федерации.

3.3. Конфиденциальная информация должна всегда оставаться собственностью Передающей стороны и без ее предварительного письменного разрешения не может копироваться или иным образом воспроизводиться Принимающей стороной.

3.4. Все документы и любые их копии, выполненные в осязаемом или электронном виде, и содержащие конфиденциальную информацию, переданную в рамках настоящего Соглашения, являются и остаются собственностью Передающей стороны независимо от того, какая из Сторон изготовила эти копии.

3.5. Ничто в настоящем Соглашении не может быть истолковано как прямое или косвенное предоставление каких-либо прав или лицензий на какое-либо изобретение, открытие или усовершенствование или каких-либо прав на обладание и/или использование какого-либо объекта интеллектуальной собственности.

3.6. При обнаружении фактов разглашения конфиденциальной информации третьим лицам Принимающая сторона обязана незамедлительно проинформировать Передающую сторону о данных фактах и предпринятых мерах по уменьшению ущерба.

4. Защита конфиденциальной информации

4.1. Принимающая сторона обязуется не разглашать полученную в рамках настоящего Соглашения конфиденциальную информацию или любую её часть любой третьей стороне без письменного разрешения обладателя этой информации.

4.2. Принимающая сторона обязуется обеспечить защиту конфиденциальной информации, полученной от Передающей стороны, от несанкционированного воздействия.

4.3. В отношении конфиденциальной информации, полученной от Передающей стороны в рамках настоящего Соглашения, Принимающая сторона обязуется:

– сохранять конфиденциальность этой информации и принимать все необходимые меры для ее защиты, по меньшей мере, с той же тщательностью, с какой она охраняет свою собственную конфиденциальную информацию;
– использовать эту информацию только в оговоренных в Соглашении целях и никогда не использовать ее в каких-либо иных целях без предварительного письменного разрешения Передающей стороны;
– не передавать эту информацию третьим сторонам без предварительного письменного разрешения Передающей стороны.

4.4. По вопросам передачи конфиденциальной информации Стороны назначают ответственного за передачу, о чем письменно уведомляют друг друга.

4.5. Передача конфиденциальной информации осуществляется по защищённым каналам связи, заказными почтовыми отправлениями, фельдъегерской или специальной связи либо работниками Сторон (нарочными). Запрещается передавать конфиденциальную информацию по открытым каналам связи, в том числе с использованием факсимильной связи и сети Интернет, без принятия соответствующих мер защиты, удовлетворяющих обе Стороны.

4.6. Передача конфиденциальной информации по Соглашению должна сопровождаться актом приема-передачи, составленным в двух экземплярах, по одному для каждой из Сторон, и подписанным уполномоченными представителями Сторон.

4.7. Принимающая сторона обязуется вернуть копии конфиденциальной информации, или уничтожить их по требованию обладателя информации с составлением акта, по форме согласованной Сторонами. Акт уничтожения полученной конфиденциальной информации составляется Принимающей стороной в двух экземплярах, по одному для каждой из Сторон, и в течение 10 (десяти) рабочих дней Принимающая сторона направляет его с сопроводительным письмом Передающей стороне.

4.8. Если третья сторона или же административные органы требуют раскрытия информации от Принимающей стороны, на основе юридических или судебных документов, Принимающая сторона обязана уведомить об этом Передающую сторону.

5. Срок действия и прекращение действия Соглашения

5.1. Соглашение прекращается по истечении срока своего действия, если Соглашение не прекращено досрочно.

5.2. Настоящее Соглашение может быть аннулировано в любое время любой Стороной путем письменного уведомления, если это не противоречит договорным обязательствам между Сторонами.

5.3. Любое прекращение действия Соглашения или истечение срока действия Соглашения не влияют на обязательства по сохранению конфиденциальности разглашённой информации в течение срока, оговоренного п. 7.10 настоящего Соглашения.

6. Судебное/государственное разглашение

6.1. Никакое положение настоящего Соглашения не может помешать Принимающей стороне раскрыть конфиденциальную информацию в том объеме, в котором она вынуждена это сделать в ответ на законные требования со стороны государственного, следственного или судебного органа в соответствии с процессуальными действиями, осуществляемыми в рамках компетенции данного органа, при условии, что перед любым таким разглашением Принимающая сторона заявит в данный орган о конфиденциальном характере данной информации.

6.2. В случае передачи конфиденциальной информации в органы или учреждения государственной власти по принуждению, Принимающая сторона обязуется ограничить эту передачу требуемым минимумом.

6.3. Принимающая сторона обязана в течении 5 (пяти) дней уведомить в письменной форме Передающую сторону о приказе или требовании о разглашении конфиденциальной информации.

6.4. Принимающая сторона обязуется оказать всестороннее содействие Передающей стороне в защите своих законных интересов, касающихся защиты конфиденциальной информации.

7. Заключительные положения

7.1. Соглашение вступает в силу со дня его подписания обеими Сторонами и действует в течение _____ лет.

7.2. Ни одна из Сторон не может переуступить свои права или обязанности по настоящему Соглашению без предварительного письменного согласия другой Стороны, и всякая намеренная переуступка без соответствующего согласия не имеет юридической силы.

7.3. Ни одна из Сторон не уполномочена действовать за или от имени другой Стороны в рамках настоящего Соглашения. Каждая Сторона является независимой Стороной в договоре и никаких партнерских или агентских отношений из настоящего Соглашения не возникает.

7.4. При нарушении одной из Сторон оговоренных в Соглашении обязательств потерпевшая Сторона вправе потребовать у виновной Стороны возмещения прямого документально подтвержденного ущерба, понесенного потерпевшей Стороной вследствие этого нарушения.

7.5. Отношения Сторон, возникшие в связи с реализацией настоящего Соглашения, регулируются законодательством Российской Федерации. Все споры, возникающие из настоящего Соглашения в связи с его толкованием или исполнением, передаются на рассмотрение в Арбитражный суд города Санкт-Петербурга и Ленинградской области.

7.6. Все уведомления или сообщения, осуществляемые в рамках настоящего Соглашения, должны быть выполнены в письменной форме, и они считаются доставленными при наличии письменного подтверждения о приеме сообщения или уведомления. Доставка уведомлений и сообщений осуществляется по указанным адресам Сторон.

7.7. В случае изменения у какой-либо из Сторон местонахождения и реквизитов данная Сторона обязана в течение 10 (десяти) рабочих дней письменно известить об этом другую Сторону.

7.8. Настоящее Соглашение составлено в двух подлинных экземплярах на русском языке.

7.9. Настоящее Соглашение представляет собой полное соглашение Сторон в отношении конфиденциальной информации, разглашаемой по настоящему Соглашению, и заменяет собой все предыдущие и подобные соглашения, уведомления, отчеты и договоренности, достигнутые Сторонами настоящего Соглашения в отношении разглашения, защиты и использования конфиденциальной информации.

7.10. Стороны обязаны соблюдать условия конфиденциальности Соглашения по отношению к ранее переданной конфиденциальной информации в течение _____ лет после окончания срока действия Соглашения.

8. Реквизиты Сторон:

Сторона 1 Сторона 2

Подписи Сторон:

Сторона 1 Сторона 2

_____/_____/ _____/_____/

М.П. М.П.