

СПб ГУТ )))	МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
	федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)
	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА
<b>СМК-ПСП-2026</b>	<b>ПОЛОЖЕНИЕ О СТРУКТУРНОМ ПОДРАЗДЕЛЕНИИ</b>



СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

**ПОЛОЖЕНИЕ**

ОБ ОТДЕЛЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Версия 1.0

Санкт-Петербург, 2026

## **1. Общие положения**

1.1. Настоящее положение об отделе информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (далее, соответственно – Положение, СПбГУТ, Университет, отдел) разработано в целях повышения эффективности трудовой деятельности работников отдела в соответствии с требованиями законодательства Российской Федерации, ГОСТ ИСО 9001-2015 и документов системы менеджмента качества Университета.

1.2. Настоящее Положение определяет основы деятельности, задачи, функции, права и ответственность работников отдела, взаимодействие с другими структурными подразделениями СПбГУТ, сторонними организациями, уполномоченными органами исполнительной власти.

1.3. Отдел является структурным подразделением СПбГУТ и подчиняется непосредственно проректору по безопасности СПбГУТ.

1.4. Отдел в своей деятельности руководствуется Конституцией Российской Федерации, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, другими нормативными правовыми документами в сфере обеспечения информационной безопасности, локальными организационно-распорядительными и нормативными документами Университета.

1.5. Отдел осуществляет свою деятельность во взаимодействии с другими структурными подразделениями СПбГУТ, а также – в пределах своей компетенции – со сторонними организациями, уполномоченными органами исполнительной власти.

## **2. Организация и структура отдела**

2.1. Штатное расписание и организационно-штатная структура отдела утверждаются приказом ректора СПбГУТ, исходя из условий и особенностей деятельности отдела, по представлению проректора по безопасности СПбГУТ.

2.2. Возглавляет отдел начальник, к прямой компетенции которого относится выполнение всех возложенных на отдел в соответствии с настоящим Положением функций и задач.

2.3. Начальник отдела назначается и освобождается от должности приказом ректора СПбГУТ по представлению проректора по безопасности СПбГУТ.

2.4. Начальник отдела несет персональную ответственность за работу отдела перед проректором по безопасности СПбГУТ.

2.5. Указания и требования начальника отдела в пределах компетенции, закрепленной его трудовым договором и должностной инструкцией, связанные с работой отдела, для работников отдела являются обязательными к исполнению.

2.6. Осуществляя руководство работниками, начальник отдела обязан:

- проявлять к подчиненным высокую требовательность, принципиальность в сочетании с уважением личного достоинства, признавая право работников иметь собственные профессиональные суждения;

- устанавливать справедливую, равномерную служебную нагрузку на работников;

- помогать работникам при возникновении у них каких-либо затруднений, оказывать морально-психологическую помощь и поддержку, вникать в запросы и нужды;

- регулировать взаимоотношения в служебном коллективе на основе принципов и норм профессиональной этики, рассматривать без промедления факты нарушения и принимать по ним объективные решения.

2.7. Работники отдела назначаются и освобождаются от должности приказом ректора СПбГУТ по представлению проректора по безопасности СПбГУТ и согласованию с начальником отдела.

2.8. Квалификационные требования, функциональные обязанности, права, ответственность работников отдела регламентируются должностными инструкциями, утверждаемыми ректором СПбГУТ.

2.9. Работа отдела ведется по плану, утвержденному проректором по безопасности СПбГУТ, в соответствии с бюджетом, утвержденным ректором СПбГУТ на год. Начальник отдела представляет проректору по безопасности СПбГУТ отчеты о работе отдела в соответствии со сроками утвержденного плана.

### **3. Основные задачи отдела**

3.1. Отдел обеспечивает информационную безопасность Университета и осуществляет деятельность по защите информационной инфраструктуры СПбГУТ и обрабатываемой в ней информации, не содержащей сведений, составляющих государственную тайну, от угроз безопасности информации.

3.2. Задачи отдела:

3.2.1. Контроль соблюдения требований и норм законодательства Российской Федерации, локальных нормативных актов Университета в области информационной безопасности;

3.2.2. Идентификация, анализ и оценка рисков информационной безопасности, а также проведение мероприятий (реализация мер) по их минимизации, включая оценку потенциальных угроз и уязвимостей;

3.2.3. Обеспечение режима информационной безопасности, включающего комплекс мер и средств, направленных на обеспечение конфиденциальности, целостности и доступности информации, защиту информационной инфраструктуры СПбГУТ от угроз безопасности информации, которые могут нанести материальный, репутационный или иной ущерб Университету.

3.2.4. Повышение уровня защищенности информационной инфраструктуры СПбГУТ;

3.2.5. Взаимодействие с уполномоченными органами исполнительной власти, сторонними организациями по вопросам, входящим в компетенцию отдела, поддержание и развитие деловых контактов, связанных с основной деятельностью отдела.

#### **4. Функции отдела**

4.1. Отдел выполняет следующие функции:

4.1.1. В рамках задачи 3.2.1:

– мониторинг законодательства и стандартов в области информационной безопасности, разработка и актуализация внутренних организационно-распорядительных и нормативно-методических документов СПбГУТ по обеспечению информационной безопасности;

– организация и проведение регулярных проверок (аудитов) информационной инфраструктуры СПбГУТ, информационных систем и процессов с целью выявления несоответствий установленным требованиям по информационной безопасности;

– исполнение предписаний Федеральной службы безопасности Российской Федерации (ФСБ России) и ее территориальных органов, Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Роскомнадзора по результатам контроля защищенности информационной инфраструктуры СПбГУТ.

4.1.2. В рамках задачи 3.2.2:

– сбор и анализ данных о состоянии информационной безопасности в СПбГУТ;

– идентификация активов в информационной инфраструктуре СПбГУТ, участие в определении ценности идентифицированных активов;

– определение угроз и уязвимостей для идентифицированных активов;

- оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов;
- участие в определении критериев принятия рисков информационной безопасности;
- планирование мероприятий по снижению уровней рисков, подготовка плана обработки рисков информационной безопасности.

#### 4.1.3. В рамках задачи 3.2.3:

- планирование и разработка мероприятий по обеспечению режима информационной безопасности при осуществлении всех видов деятельности СПбГУТ, исключая работы со сведениями, составляющими государственную тайну;
- организация и проведение мероприятий по обеспечению в СПбГУТ действенного режима информационной безопасности при обработке, хранении и передаче информации с использованием средств вычислительной техники, средств телекоммуникаций и иных технических средств, а также в процессе документационного обеспечения деятельности Университета, подготовка соответствующих отчетных документов;
- мониторинг событий информационной безопасности в информационной инфраструктуре СПбГУТ, анализ событий, произошедших на объектах информатизации по различным системным журналам, включая данные систем мониторинга событий информационной безопасности;
- контроль конфигураций, учетных записей, прав доступа к информационной инфраструктуре СПбГУТ, предотвращение несанкционированного доступа к защищаемой информации;
- контроль действий пользователей и администраторов автоматизированных и информационных систем СПбГУТ на предмет соблюдения ими требований режима информационной безопасности;
- обнаружение и предупреждение компьютерных атак, участие в ликвидации последствий компьютерных атак, реагирование на инциденты информационной безопасности;
- анализ состояния системы защиты информации СПбГУТ с целью выявления и устранения слабых мест в ее организации;
- инструментальное тестирование информационных ресурсов, автоматизированных и информационных систем СПбГУТ на наличие уязвимостей, участие в устранении выявленных уязвимостей;
- выявление в информационной инфраструктуре СПбГУТ возможных каналов утечки сведений, составляющих охраняемую законами Российской Федерации тайну, участие в устранении выявленных нарушений требований режима информационной безопасности;
- проведение мероприятий по предупреждению нарушений требований режима информационной безопасности при обработке информации в информационной инфраструктуре СПбГУТ;

- методическое руководство, координация и контроль деятельности структурных подразделений СПбГУТ по вопросам организации и проведения мероприятий по обеспечению режима информационной безопасности и защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну;

- установка, контроль и системное администрирование средств защиты информации на объектах информатизации структурных подразделений СПбГУТ, включая средства криптографической защиты информации;

- организация аттестаций объектов информатизации СПбГУТ, предназначенных для обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, на соответствие требованиям по информационной безопасности;

- участие в проведении служебных разбирательств по фактам нарушений режима информационной безопасности, разглашения охраняемой законами Российской Федерации тайны, утраты либо хищения носителей таких сведений в структурных подразделениях СПбГУТ, исключая работы со сведениями, составляющими государственную тайну;

- участие в рассмотрении и согласовании технических заданий, научно-исследовательских, опытно-конструкторских и иных работах по вопросам, входящим в компетенцию отдела, исключая работы со сведениями, составляющими государственную тайну;

- организация и проведение в установленном порядке проверок структурных подразделений СПбГУТ по вопросам, входящим в компетенцию отдела, подготовка соответствующих отчетных документов;

- формирование и контроль затрат, отнесенных к компетенции отдела, формирование заявок на включение сведений в план-график закупок (расходов) на плановый период по направлению деятельности отдела;

- подготовка отчетов о состоянии информационной безопасности в СПбГУТ.

#### 4.1.4. В рамках задачи 3.2.4:

- анализ и оценка состояния защищенности информационной инфраструктуры Университета, разработка предложений по совершенствованию системы защиты информации в СПбГУТ;

- экспертиза инициатив, проектов и решений в области информационной безопасности на предмет необходимости и целесообразности их реализации в Университете;

- внедрение, модернизация, замена средств защиты информации;

- изучение и обобщение научно-технической литературы, нормативных и методических материалов по техническим средствам и способам защиты информации;

- исследование функциональных возможностей, технических характеристик, принципов работы технических средств и программного обеспечения, применяемых для защиты информации;
- исследование технологий обработки информации для определения необходимости и достаточности защиты на объектах информатизации;
- разработка (актуализация) и внедрение нормативных и распорядительных документов по информационной безопасности.

#### 4.1.5. В рамках задачи 3.2.5:

- обеспечение взаимодействия с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) по вопросам, входящим в компетенцию отдела;
- обеспечение взаимодействия с уполномоченными органами исполнительной власти (ФСБ России, ФСТЭК России, Роскомнадзор) в рамках защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну;
- участие в ведомственных и межведомственных проверках уполномоченных федеральных органов исполнительной власти и других контролирующих организаций по вопросам информационной безопасности;
- обеспечение взаимодействия с организациями – поставщиками решений и услуг в сфере информационной безопасности.

### **5. Права работников отдела**

Работники отдела в процессе своей деятельности имеют следующие права:

5.1. Запрашивать от любых должностных лиц и структурных подразделений любую информацию, необходимую им для выполнения своих должностных обязанностей.

5.2. Пользоваться в установленном порядке бухгалтерской, бюджетной, статистической и иной отчетностью СПБГУТ по вопросам, входящим в компетенцию отдела.

5.3. Издавать в пределах своей компетенции инструктивные документы и готовить проекты распорядительных документов.

5.4. По согласованию с руководством СПБГУТ инициировать и проводить внутренние проверки выполнения требований информационной безопасности в структурных подразделениях СПБГУТ, в том числе с использованием аппаратно-программных средств.

5.5. Получать доступ к информационным ресурсам СПБГУТ, необходимый для выполнения отделом своих функций.

5.6. В установленном порядке организовывать и контролировать внесение изменений в работу или изменение режимов функционирования средств защиты информации, оборудования, информационных систем,

системного и прикладного программного обеспечения, входящего в состав информационной инфраструктуры СПбГУТ.

5.7. Требовать прекращения (приостановки) работ (в случае нарушений, несоблюдения установленных требований и т.д.), соблюдения установленных норм, правил, инструкций, давать рекомендации по исправлению недостатков и устранению нарушений.

5.8. Привлекать с согласия руководителей структурных подразделений работников иных подразделений для осуществления мероприятий, проводимых отделом в соответствии с возложенными на него задачами.

5.9. Вести переписку (в том числе с использованием электронных каналов связи) и представлять в установленном порядке от имени СПбГУТ, по согласованию с ректором или лицом, его замещающим.

5.10. Начальник отдела вправе принимать участие в совещаниях, проводимых по вопросам, связанным с деятельностью отдела.

5.11. Работники отдела имеют также и иные права, закрепленные в их должностных инструкциях.

## **6. Взаимодействие с другими подразделениями**

6.1. Отдел получает:

- от проректора по безопасности СПбГУТ: приказы, распоряжения, согласования и другие документы административного, управленческого и информационного характера;

- от структурных подразделений СПбГУТ: согласования, информацию, материальные и нематериальные ресурсы, связанные с деятельностью отдела, заявки на обеспечение сервисами и услугами в части деятельности отдела;

- от департамента безопасности и режима: методические рекомендации и распоряжения касающейся пропускного режима и экономической безопасности в отношении деятельности отдела;

- от отдела технической защиты информации: методические рекомендации и распоряжения в части, касающейся защиты информации ограниченного доступа, за исключением информации, содержащей сведения, составляющие государственную тайну.

6.2. Отдел передает:

- проректору по безопасности СПбГУТ: отчеты, заявки, плановую, бюджетную и иную информацию по деятельности отдела;

- структурным подразделениям СПбГУТ: информацию в соответствии с задачами и функциями отдела;

6.3. Взаимоотношения отдела со сторонними организациями, органами исполнительной власти регламентируются законодательством, уставом СПбГУТ.

## 7. Ответственность работников отдела

7.1 Всю полноту ответственности за качество и своевременность выполнения задач, возложенных на отдел, несет начальник отдела

7.2 На начальника отдела возлагается персональная ответственность за:

- соблюдение законодательства Российской Федерации;
- выполнение возложенных на отдел функций и задач;
- своевременное и качественное выполнение приказов руководства СПбГУТ;
- рациональное и эффективное использование материальных, финансовых и кадровых ресурсов;
- ведение установленной документации;
- предоставление в установленном порядке достоверной статистической и иной информации о деятельности отдела;
- готовность отдела к работе в условиях чрезвычайных ситуаций;
- надлежащее функционирование и целевое использование аппаратных и аппаратно-программных систем и комплексов, предназначенных для обеспечения режима информационной безопасности, исключая работы со сведениями, составляющими государственную тайну;
- полноту и правильность использования предоставленных прав в интересах достижения трудовой дисциплины, производительности труда и качественного выполнения работ в установленные сроки;
- выполнение требований документов системы менеджмента качества в соответствии с закреплёнными функциями;
- выполнение требований в области защиты информации ограниченного доступа, в том числе персональных данных в СПбГУТ, за исключением информации, содержащей сведения, составляющие государственную тайну;
- соблюдение стандартов, правил, норм и инструкций по охране труда, пожарной безопасности, требований по экологической безопасности;
- своевременность исполнения запланированных работ и оказания услуг по номенклатуре отдела.

7.3. Степень ответственности других работников отдела устанавливается их должностными инструкциями и ограничена прямым действительным ущербом в соответствии с действующим трудовым законодательством России при условии наличия их прямой вины.