

**Опрос работодателей о значимости и ожидаемой результативности
подготовки обучающихся в СКТ(ф)СПбГУТ по специальности 10.02.04
Обеспечение информационной безопасности телекоммуникационных систем**

в опросе приняли участие предприятия-партнеры:

Смоленский филиал ПАО "Ростелеком"

ООО Твинс (WebCanare)

АО "НИИ СТТ"

ООО "Смолтелеком"

ОГАУЗ "СОМИАЦ" (СОГАУ "ЦИТ")

ООО "Смоленсксвязстрой"

Смоленское региональное отделение СЗФПАО "МегаФон"

Профессиональные модули	Профессиональные компетенции (обучающиеся, освоившие образовательную программу, должны обладать ПК)	Значимость полученных знаний и практических навыков
ВД.01 Эксплуатация информационно-телекоммуникационных систем и сетей	ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей. ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей. ПК 1.3. Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей. ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.	Эффективная эксплуатация информационно-телекоммуникационных систем и сетей включающая знание и принципы работы: 1. Приемо-передающих устройств, линейных сооружений связи и источников. 2. Телекоммуникационных систем и сетей. 3. Электрорадиоизмерений и метрологии.
ВД.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты	ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей. ПК 2.2. Поддерживать	Знание различных видов защиты информации в информационно-телекоммуникационных системах и сетях позволяют осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных

	бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях. ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.	системах и сетях.
ВД.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях. ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях. ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями. ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.	Защита информации в информационно-телекоммуникационных системах и сетях производится не только с помощью программно-аппаратных средств защиты, но и с использованием технических средств защиты, при этом особое место имеет физическая защита линий связи информационно-телекоммуникационных систем и сетей.

Ожидания работодателей от специалистов:

Важность информационной безопасности заключается в том, что она обеспечивает защиту информации от несанкционированного доступа, изменений и уничтожения.

Важность информационной безопасности в разрезе решаемых задач:

Для бизнеса:

Эффективная система защиты корпоративных данных предотвращает утечки информации, конфиденциальные нарушения и финансовые потери.

Также меры по безопасности помогают избежать проблем с законодательством и сохраняют репутацию компании.

Для государственных структур:

Защита электронных финансовых транзакций, важных коммуникационных систем и критической инфраструктуры становится ключевым аспектом обеспечения стабильности государства.

Для личной безопасности:

Защита умных устройств, маршрутизаторов и персональных компьютеров от кибератак обеспечивает безопасное использование цифровых технологий в повседневной жизни.

Нарушение информационной безопасности может привести к серьёзным последствиям, включая финансовые потери, потерю конфиденциальности, ущерб репутации и даже угрозу безопасности государства.