

**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)**

Утверждаю
Первый проректор – проректор
по учебной работе
_____ А.В. Абилов
18.01.2024

**ПРОГРАММА ВСТУПИТЕЛЬНЫХ ИСПЫТАНИЙ
ДЛЯ ПОСТУПАЮЩИХ
НА БАЗЕ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ,
НА НАПРАВЛЕНИЕ ПОДГОТОВКИ
10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
10.05.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ
10.05.07 ПРОТИВОДЕЙСТВИЕ ТЕХНИЧЕСКИМ РАЗВЕДКАМ
ПРОФЕССИОНАЛЬНО-ПРИКЛАДНЫЕ КОМПЕТЕНЦИИ ПО
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Санкт-Петербург
2024

Тема 1: Основы теории информации

1. Основные понятия теории информации: источник, носитель и получатель информации, сигнал, параметры сигнала (дискретность или непрерывность), измерение информации
2. Вероятностный подход к измерению информации; формулы Хартли и Шеннона
3. Понятие пропускной способности информационных каналов связи.
4. Понятие скорости передачи информации, единицы ее измерения. Передача информации техническими средствами коммуникаций

Тема 2: Основы программирования

1. Способы описания алгоритмов. Средства графического изображения алгоритмов
2. Программа. Компиляция и исполнение программы (на примере любого ЯВУ)
3. Идентификаторы и служебные слова (на примере любого ЯВУ)
4. Арифметические и логические операции (на примере любого ЯВУ)
5. Типы данных (на примере любого ЯВУ)
6. Форматный и потоковый ввод-вывод данных (на примере любого ЯВУ)
7. Программирование ветвлений (на примере любого ЯВУ)
8. Программирование циклов (на примере любого ЯВУ)
9. Указатели и массивы (на примере любого ЯВУ)
10. Функции (на примере любого ЯВУ)

Тема 3: Основы информационной безопасности

1. Понятие информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.
3. Понятие «угроза информации».
4. Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий.
5. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
6. Целостность, доступность и конфиденциальность информации.
7. Классификация информации по видам тайны и степеням конфиденциальности.
8. Понятия государственной тайны и конфиденциальной информации.
9. Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации.
10. Каналы и методы несанкционированного доступа к уязвимости информации.
11. Методы оценки уязвимости информации
12. Российские и международные стандарты, определяющие требования к защите информации.
13. Система сертификации РФ в области защиты информации. Основные

правила и документы системы сертификации РФ в области защиты информации

14. Основные механизмы защиты информации.
15. Система защиты информации.
16. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.
17. Программные и программно-аппаратные средства защиты информации
18. Инженерная защита и техническая охрана объектов информатизации
19. Организационно-распорядительная защита информации.
20. Работа с кадрами и внутриобъектовый режим.
21. Аттестация объектов информатизации по требованиям безопасности информации. Основные понятия в области аттестации по требованиям безопасности информации и их определения.
22. Системы сертификации средств защиты информации по требованиям безопасности информации.
23. Технологии разграничения доступа
24. Концепция построения виртуальных защищенных сетей
25. Технологии обнаружения вторжений

Ответственный секретарь ПК



С.И. Ивасишин