Федеральное государственное автономное образовательное учреждение высшего образования
«Санкт-Петербургский политехнический университет Петра Великого»

УТВЕРЖДАЮ
Директор ИКНК
_____ Д.П. Зегжда
«17» июня 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«Защита информации»

Разработчик	Высшая школа компьютерных технологий и информационных систем
Направление (специальность) подготовки	09.03.01 Информатика и вычислительная техника
Наименование ООП	09.03.01_01 Разработка компьютерных систем
Квалификация (степень) выпускника	**бакалавр**
Образовательный стандарт	**СУОС**
Форма обучения	**Очная**

СОГЛАСОВАНО
Руководитель ОП
_____ Р.В. Цветков
«26» марта 2024 г.

Соответствует СУОС
Утверждена протоколом заседания высшей школы "ВШКТиИС"
от «26» марта 2024 г. № 1

РПД разработал:
Доцент, к.т.н., доц. В.А. Сушников

1. Цели и планируемые результаты изучения дисциплины

Цели освоения дисциплины

Подготовка студента к деятельности, связанной с использованием современных информационных систем, с учётом требований по защите информации.

Результаты обучения выпускника

Код	Результат обучения (компетенция) выпускника ООП
ПК-1	**Способен использовать интеллектуальные технологии для проектирования сложных технических систем**
ИД-1 ПК-1	Применяет современные информационные технологии при создании технических систем
ПК-3	**Способен проектировать специализированные цифровые и аналоговые элементы и устройства вычислительной техники**
ИД-2 ПК-3	Проводит оценочный расчет требований к характеристикам отдельных блоков с целью детализации технического задания
ИД-3 ПК-3	Разрабатывает электрические схемы отдельных аналоговых, цифровых и смешанных блоков устройства
ИД-4 ПК-3	Выполняет комплексирование и наладку устройства в соответствии с разработанным проектом
ПК-5	**Способен интегрировать систему-на-кристалле (СнК) в программно-аппаратную систему**
ИД-1 ПК-5	Определяет состав элементов и их параметров для системного окружения СнК
ИД-2 ПК-5	Выполняет конструирование печатной платы модуля, включающего СнК

Планируемые результаты изучения дисциплины

знания:

- стандарты ввода/ вывода современных интегральных схем и их номенклатуру
- требования к конструкции печатных плат
- основные характеристики типовых блоков
- принципы и стандарты конструирования и обеспечения электромагнитной совместимости
- основные методики проведения наладки электронных устройств

- спектр инструментальных средств, пригодных для использования на разных стадиях проектирования программного обеспечения

умения:

- создавать схему устройства с СнК
- создавать топологию для схемы устройства с СнК
- производить оценочные расчеты основных параметров типовых блоков
- конструировать электронные устройства с высокой помехоустойчивостью
- использовать современные контрольно-измерительные приборы при проведении наладки
- обоснованно выбирать набор инструментальных средств для обеспечения процесса разработки программных систем

навыки:

- использование средств автоматизированного проектирования для ввода схем уровня печатной платы
- использование средств автоматизированного проектирования для разводки печатной платы
- владение методикой расчета параметров основных функциональных узлов
- владение программными средствами сквозного проектирования (разработка, моделирование, изготовление)
- владение методиками проведения наладки электронных устройств
- использование средств автоматизированного проектирования для ввода схем уровня печатной платы

2. Место дисциплины в структуре ООП

В учебном плане дисциплина «Защита информации» относится к модулю «Модуль цифровых компетенций».

Изучение дисциплины базируется на результатах освоения следующих дисциплин:

- Технологии компьютерных сетей

3. Распределение трудоёмкости освоения дисциплины по видам учебной работы и формы текущего контроля и промежуточной аттестации

3.1. Виды учебной работы

Виды учебной работы	Трудоемкость по семестрам
	Очная форма
Лекционные занятия	20
Лабораторные занятия	20
Самостоятельная работа	41
Часы на контроль	16
Промежуточная аттестация (экзамен)	11
Промежуточная аттестация (зачет)	0
Общая трудоемкость освоения дисциплины	108, ач
	3, зет

3.2. Формы текущего контроля и промежуточной аттестации

Формы текущего контроля и промежуточной аттестации	Количество по семестрам
	Очная форма
Текущий контроль	
Контрольные, шт.	1
Промежуточная аттестация	
Экзамены, шт.	1

4. Содержание и результаты обучения

4.1 Разделы дисциплины и виды учебной работы

№ раздела	Разделы дисциплины, мероприятия текущего контроля	Очная форма		
		Лек, ач	Лаб, ач	СР, ач
1.	Введение. Основные понятия и определения.	1	0	4

2.	Законодательное обеспечение. Законы, указы, стандарты, нормативные документы	1	0	2
3.	Классификация информационных ресурсов, угрозы, нарушители, риски	2	0	2
4.	Политика безопасности	2	0	4
5.	Организационные меры защиты информации (процедурный уровень)	2	0	2
6.	Программно-технический уровень защиты информации	2	4	3
7.	Основы криптографической защиты информации	2	3	2
8.	Межсетевое экранирование	2	4	2
9.	Виртуальные частные сети	2	4	2
10.	Вредоносное ПО и меры противодействия	2	2	8
11.	Сканеры безопасности, системы обнаружения вторжений, DLP системы	2	3	10
Итого по видам учебной работы:		20	20	41
Экзамены, ач				16
Часы на контроль, ач				16
Промежуточная аттестация (экзамен)		11		
Общая трудоёмкость освоения: ач / зет		108 / 3		

4.2. Содержание разделов и результаты изучения дисциплины

Раздел дисциплины	Содержание
1. Введение. Основные понятия и определения.	Структура дисциплины. Основные цели и задачи. Общие понятия обеспечения информационной безопасности. Проблема безопасности компьютерной информации. Термины.
2. Законодательное обеспечение. Законы, указы, стандарты, нормативные документы	Нормативные документы: законы, стандарты, руководящие материалы ФСТЭК. Система сертификации и лицензирования
3. Классификация информационных ресурсов, угрозы, нарушители, риски	Классификация информации и ресурсов. Источники угроз компьютерной информации. Классификация угроз. Модель нарушителя. Основные понятия оценки и управления рисками компьютерной информации. Виды и особенности атак на компьютерную информацию
4. Политика безопасности	Понятие политики безопасности. Назначение и состав политики безопасности. Виды частных политик безопасности.
5. Организационные меры защиты информации (процедурный уровень)	Управление персоналом. Управление физическим доступом. Поддержание работоспособности. Реакция на нарушение режима безопасности. Расследование инцидентов. Планирование восстановительных работ
6. Программно-технический уровень защиты информации	Базовые сервисы. Идентификация и аутентификация. Управление доступом (произвольное, принудительное, ролевое). Протоколирование и аудит, системы корреляции событий. Восстановление
7. Основы криптографической защиты информации	Симметричное шифрование, основные алгоритмы. Ассиметричное шифрование, открытый и закрытый ключи, распределение ключей. Хеш функция, электронная подпись, сертификаты, PKI.
8. Межсетевое экранирование	Межсетевые экраны, классификация, принципы работы, используемые технологии (пакетный фильтр, инспектор состояний, nat, посредники сеансового и прикладного уровня). Примеры решений различных производителей
9. Виртуальные частные сети	Построение защищенных сетей. Элементы VPN. Основные протоколы реализации VPN. Протокол IPSec. Основные типы защищенных связей. Состав и назначение сертификатов. Организация центров сертификации. Примеры отечественных систем, реализующих VPN.

10. Вредоносное ПО и меры противодействия	Вредоносные программы. Классификация: вирусы, сетевые черви, троянские программы. Основные способы распространения. Меры противодействия, особенности использования в корпоративной среде. Основные вендоры.
11. Сканеры безопасности, системы обнаружения вторжений, DLP системы	Сканеры, принцип действия, системы обнаружения вторжений, классификация, принцип действия, примеры систем. DLP системы, классификация, принцип действия

5. Образовательные технологии

1. Основной материал дисциплины студенты изучают на лекциях. Основные темы подкрепляются лабораторными работами и практическими занятиями, часть из которых выполняются в интерактивном режиме. Дополнительная информация по дисциплине предоставляется в виде: ссылок на главы основной и дополнительной литературы; описания заданий на практические занятия; статьи, раскрывающие современное состояние рассмаириваемых вопросов; ссылки на сайты, содержащие обзоры, свободно распространяемые программные продукты и их описания.
2. Лекции по курсу проводятся в форме презентации. Материалы презентаций рассылаются студентам заблаговременно. В отдельных случаях материалы презентаций дополнены приложениями, в которых изложены справочные материалы и таблицы, дополнительные сведения по теме, определения, вспомогательные формулы, материалы обзоров.
3. При подготовке к экзамену проводится специальное занятие с использованием электронных ресурсов и подробным разбором примеров контрольных экзаменационных вопросов.
4. Элементы технологии Case-study. Индивидуальные задания к лабораторным и практическим занятиям содержат описания практических проблем
5. Опережающая самостоятельная работа. Подготовка к лабораторным занятиям предполагает самостоятельное изучение организации МПК и лабораторного стенда, программы работы.
6. Исследовательский метод. Индивидуальные задания к лабораторным занятиям формулируются преподавателями в виде, предполагающем творческий поиск и применение знаний, полученных в других курсах обучения.
7. Обучение на основе опыта. При проведении лекций и лабораторных занятий предполагается изложение многочисленных примеров из практики преподавателей.

6. Лабораторный практикум

№ раздела	Наименование лабораторных работ	Трудоемкость, ач
		Очная форма
1.	Анализ безопасности персонального компьютера и меры по усилению защиты.	2
2.	Анализ трафика в компьютерной сети	2
3.	Защита сети с использованием межсетевых экранов.	2
4.	Обнаружение сетевых атак с помощью системы обнаружения вторжений Snort	2
5.	Анализ защищённости с использованием Zenmap и Xspider	2
6.	Настройка VPN на базе IPsec	6
7.	Изучение возможностей программы Gpg4win	4
	Итого часов	20

7. Практические занятия

Не предусмотрено

8. Организация и учебно-методическое обеспечение самостоятельной работы

Примерное распределение времени самостоятельной работы студентов

Вид самостоятельной работы	Примерная трудоемкость, ач
	Очная форма
Текущая СР	
работа с лекционным материалом, с учебной литературой	9
опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	6
самостоятельное изучение разделов дисциплины	8
выполнение домашних заданий, домашних контрольных работ	0
подготовка к лабораторным работам, к практическим и семинарским занятиям	6
подготовка к контрольным работам, коллоквиумам	6
Итого текущей СР:	35
Творческая проблемно-ориентированная СР	
выполнение расчётно-графических работ	0
выполнение курсового проекта или курсовой работы	0
поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	6
работа над междисциплинарным проектом	0
исследовательская работа, участие в конференциях, семинарах, олимпиадах	0
анализ данных по заданной теме, выполнение расчётов, составление схем и моделей на основе собранных данных	0
Итого творческой СР:	6
Общая трудоемкость СР:	41

9. Учебно-методическое обеспечение дисциплины

9.1. Адрес сайта курса

https://dl.spbstu.ru/course/view.php?id=2735

9.2. Рекомендуемая литература

Основная литература

№	Автор, название, место издания, издательство, год (годы) издания	Год изд.	Источник
1	Нестеров С.А. Основы информационной безопасности: Санкт-Петербург: Изд-во Политехн. ун-та, 2014. URL: http://elib.spbstu.ru/dl/2/4744.pdf	2014	ЭБ СПбПУ

Ресурсы Интернета

1. Граничин О., Кияев В. Безопасность информационных систем: https://www.intuit.ru/studies/courses/13845/1242/info
2. Мэйволд Э. Безопасность сетей: https://www.intuit.ru/studies/courses/102/102/info
3. Жданов О., Ушаков Ю. Криптографические методы защиты информации: https://www.intuit.ru/studies/courses/13837/1234/info
4. Лапонина О. Межсетевые экраны: https://www.intuit.ru/studies/courses/14250/1286/info
5. Галатенко В. Основы информационной безопасности: https://www.intuit.ru/studies/courses/10/10/info

9.3. Технические средства обеспечения дисциплины

Электронные презентации и документы по разделам курса.

При провелении лабораторных работ используются специализированные программы Wireshark, Nmap, Xspider, Kleopatra

10. Материально-техническое обеспечение дисциплины

Занятия проводятся в специализированном классе, включающем локальную сеть Ethernet, подключенную к Internet. На каждом рабочем месте – персональный компьютер (ОС Win). Используются программы tcpdump, WireShark, snort, Nmap, специализированные МЭ.

11. Критерии оценивания и оценочные средства

11.1. Критерии оценивания

Для дисциплины «Защита информации» формой аттестации является экзамен. Дисциплина реализуется с применением системы индивидуальных достижений.

Текущий контроль успеваемости

Максимальное значение персонального суммарного результата обучения (ПСРО) по приведенной шкале - 100 баллов
Максимальное количество баллов приведенной шкалы по результатам прохождения двух точек контроля - 80 баллов.

Подробное описание правил проведения текущего контроля с указанием баллов по каждому контрольному мероприятию и критериев выставления оценки размещается в СДО в навигационном курсе дисциплины.

Промежуточная аттестация по дисциплине

Максимальное количество баллов по результатам проведения аттестационного испытания в период промежуточной аттестации – 20 баллов приведенной шкалы.

Промежуточная аттестация по дисциплине проводится в соответствии с расписанием.

Оценки «отлично» заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложения и использовании учебно-программного материала.

Результаты промежуточной аттестации, определяются на основе баллов, набранных в рамках применения, СИД

Баллы по приведенной шкале в рамках применения СИД (ПСРО+ ПА)	Оценка по результатам промежуточной аттестации
	Экзамен/диф.зачет/зачет
0 - 60 баллов	Неудовлетворительно/не зачтено
61 - 75 баллов	Удовлетворительно/зачтено
76 - 89 баллов	Хорошо/зачтено
90 и более	Отлично/зачтено

11.2. Оценочные средства

Оценочные средства по дисциплине представлены в фонде оценочных средств, который является неотъемлемой частью основной образовательной программы и размещается в электронной информационно-образовательной среде СПбПУ на портале etk.spbstu.ru

12. Методические рекомендации по организации изучения дисциплины

Данная дисциплина использует ранее полученные студентами знания о принципах построения и использования средств аппаратного и программного обеспечения в компьютерных сетях, о работе компьютерных сетей.

Основной материал излагается на лекциях, посещение лекционных занятий контролируется. В качестве дополнения студентам рекомендуются использовать образовательные ресурсы на платформах openedu, **coursera.org**, intuit.ru

Каждое практическое занятие ориентировано на подкрепление лекционного материала, получение дополнительных знаний и практических навыков в использовании средств защиты. Каждое задание на практическое занятие включает список вопросов, на которые дается ответ в отчете. Выполнение задания практического занятия может потребовать самостоятельного изучения рекомендованной литературы. По ряду разделов курса, вынесенных на самостоятельное изучение, студенты пишут рефераты, которые потом обсуждаются на практических занятиях.

Контроль усвоения изученного материала осуществляется посредством защиты студентами отчетов по практическим занятиям, практически закрепляющих полученные знания. Итоговая аттестация производится в ходе устного экзамена по дисциплине.

13. Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-

медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.