

Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)

УТВЕРЖДАЮ
Директор ВШТЭ



Рабочая программа дисциплины

Б1.В.ДВ.01.02 Информационная безопасность

Учебный план: _____ ФГОС3++b130301ПТ-1234_26-14.plx

Кафедра: 16 Прикладной математики и информатики

Направление подготовки:
(специальность) 13.03.01 Теплоэнергетика и теплотехника

Профиль подготовки:
(специализация) Промышленная теплоэнергетика

Уровень образования: бакалавриат

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоё мкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия				
5	УП	17	17	37,75	0,25	2	Зачет
	РПД	17	17	37,75	0,25	2	
Итого	УП	17	17	37,75	0,25	2	
	РПД	17	17	37,75	0,25	2	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 13.03.01 Теплоэнергетика и теплотехника, утверждённым приказом Минобрнауки России от 28.02.2018 г. № 143

Составитель (и):

старший преподаватель

Маслобоев А.Н.

От кафедры составителя:

Заведующий кафедрой прикладной математики и информатики

Ремизова И.В.

От выпускающей кафедры:

Заведующий кафедрой

Громова Е.Н.

Методический отдел:

Фахретдинова А. Р.

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: формирование компетенции в области разработки системы защиты информации организации на основе оценки существующих угроз безопасности и современных методик определения эффективности подобных систем.

1.2 Задачи дисциплины:

- усвоение основ информационной безопасности — источников, рисков и форм атак на информацию;
- усвоение знаний в области политики и стандартов информационной безопасности;
- ознакомление с основами криптографии и средствами антивирусной защиты;
- изучение показателей и методик эффективности системы защиты информации;
- установление состава мероприятий по обеспечению функционирования комплексной системы защиты информации.

1.3 Требования к предварительной подготовке обучающегося:

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-5.1: Способен выполнять специальные расчеты теплотехнологических процессов по типовым методикам
Знать: номенклатуру нормативных документов в области профессиональной деятельности; основные понятия информационной безопасности; основные принципы функционирования систем безопасности в современных операционных системах и оболочках; возможности применения в работе современных системных программных средств
Уметь: анализировать информационную безопасность многопользовательских систем; пользоваться программными средствами, реализующими основные криптографические функции-системы публичных ключей, цифровую подпись, разделение доступа.
Владеть: современной терминологией и методологией в области информационной безопасности.

3 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Форма текущего контроля
		Лек. (часы)	Пр. (часы)		
Раздел 1. Основные понятия и определения	5				О
Тема 1. Основные составляющие информационной безопасности Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Сценарии реализации угроз информационной безопасности. Внутренние угрозы информационной безопасности. Важность и сложность проблем защиты информации в ИС.		2	1	2,5	
Тема 2. Законодательный уровень информационной безопасности. Законодательные и правовые основы защиты компьютерной информации информационных технологий. Обзор российского законодательства в области информационной безопасности. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС		3	1	2	
Раздел 2. Криптографическая защита информации					О
Тема 3. Основные принципы криптографической защиты информации Понятие криптографии. Понятия о симметричных и асимметричных криптосистемах. Понятие криптоанализа. Аппаратно-программные криптографические средства защиты информации. Системы идентификации и аутентификации пользователей. Системы шифрования данных.		4	3	7,25	
Тема 4. Асимметричные криптосистемы Концепция криптосистемы с открытым ключом. Однонаправленные функции. Криптосистема шифрования данных RSA. Процедуры шифрования и расшифрования в криптосистеме RSA. Безопасность и быстродействие криптосистемы RSA. Аутентификация данных и электронная цифровая подпись		2	3	6	

Тема 5. Симметричные криптосистемы Понятие о симметричной криптосистеме. Шифры перестановки. Шифрующие таблицы. Система шифрования Цезаря. Шифры сложной замены. Шифрование методом гаммирования. Стандарт шифрования данных DES.		2	3	6	
Раздел 3. Защита информации в компьютерных сетях					
Тема 6. Обеспечение безопасности систем, входящих в состав глобальных компьютерных сетей. Понятие межсетевого экрана (firewall). Экраны прикладного уровня. Экраны с пакетной фильтрацией. Гибридные межсетевые экраны. Организация и эксплуатация виртуальных частных сетей (VPN). Пользовательские и узловые VPN. Системы предотвращения вторжений (IDS). Узловые и сетевые IDS.		2	3	6	О
Тема 7. Обеспечение безопасного взаимодействия в глобальных компьютерных сетях Управление ключами и сертификация ключей. Концепция доверия в информационной системе. Иерархическая модель доверия. Сетевая модель доверия. Протокол конфиденциального обмена данными SSL. Обеспечение безопасности беспроводных сетей. Обеспечение безопасности электронной почты.		2	3	8	
Итого в семестре (на курсе для ЗАО)		17	17	37,75	
Консультации и промежуточная аттестация (Зачет)		0,25			
Всего контактная работа и СР по дисциплине		34,25		37,75	

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5 БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ

Использование балльно-рейтинговой системы не предусмотрено.

6. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ, КРИТЕРИЕВ, СИСТЕМЫ И СРЕДСТВ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

6.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения
ПК-5.1	1. Имеет базовые знания об использовании современных средств защиты информации 2. Демонстрирует навыки применения современных антивирусных средств и методов криптографии для защиты информации 3. Свободно ориентируется в современной терминологии в области информационной безопасности

6.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
Зачтено	Обучающийся твердо знает материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопросы, способен правильно применить основные методы и инструменты при решении практически задач, владеет необходимыми навыками и приемами их выполнения	
Не зачтено	Обучающийся знает материал не в полном объеме, или же вообще его не знает. Изложение материала страдает от неграмотности и от объяснения мелких деталей вопроса, не показывая ответ по существу. Обучающийся допускает существенные неточности в ответе на вопросы, не способен правильно применить основные методы и инструменты при решении практических задач, абсолютно не владеет необходимыми навыками и приемами их выполнения.	

6.3 Типовые контрольные задания и/или иные материалы, используемые для оценки результатов обучения

6.3.1 Типовые контрольные вопросы

№ п/п	Формулировки вопросов
Семестр 5	
1	Методы и средства защиты информации.
2	Организационное обеспечение информационной безопасности
3	Организация конфиденциального делопроизводства.
4	Комплекс организационно-технических мероприятий по обеспечению защиты информации.
5	Инженерно-техническое обеспечение компьютерной безопасности.
6	Защита информации в Интернете
7	Защита от компьютерных вирусов.
8	Популярные антивирусные программы и их классификация.
9	Организация системы защиты информации экономических объектов.
10	Криптографические методы защиты информации.
11	Этапы построения системы защиты информации.
12	Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
13	Основные понятия информационной безопасности.
14	Система защиты информации и ее структура
15	Информация как товар и объект безопасности.
16	Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
17	Персональные данные и их защита.
18	Информационные угрозы, их виды и причины возникновения.
19	Способы воздействия информационных угроз на объекты.
20	Внешние и внутренние субъекты информационных угроз.
21	Вредоносные программы, их виды.
22	История компьютерных вирусов и современность.
23	Политика безопасности и ее принципы.
24	Фрагментарный и системный подход к защите информации

6.3.2 Типовые тестовые задания

Не предусмотрено

6.3.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Разработать в современной среде объектно-ориентированного программирования приложение, реализующее шифр Цезаря

2. Используя шифр Виженера, зашифровать фразу "электронная цифровая подпись". В качестве ключевого слова использовать свое полное имя

6.4 Методические материалы, определяющие процедуры оценивания результатов обучения

6.4.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

6.4.2 Форма проведения промежуточной аттестации по дисциплине

Устная ☐ Письменная ☐ Компьютерное тестирование ☐ Иная ☐

6.4.3 Особенности проведения промежуточной аттестации по дисциплине

Время на подготовку к ответу по билету - 30 минут.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
7.1.1 Основная учебная литература				
Фомин, Д. В.	Информационная безопасность	Саратов, Москва: Профобразование, Ай Пи Ар Медиа	2022	https://www.iprbooks.hop.ru/118458.html
Ревнивых, А. В.	Информационная безопасность организаций	Москва: Ай Пи Ар Медиа	2021	https://www.iprbooks.hop.ru/108227.html
7.1.2 Дополнительная учебная литература				
Куликов, С. С.	Информационная безопасность локальных компьютерных сетей	Воронеж: Воронежский государственный технический университет, ЭБС АСВ	2021	https://www.iprbooks.hop.ru/118614.html
Куликов, С. С.	Информационная безопасность глобальных компьютерных сетей	Воронеж: Воронежский государственный технический университет, ЭБС АСВ	2021	https://www.iprbooks.hop.ru/118613.html

7.2 Перечень профессиональных баз данных и информационно-справочных систем

Электронно-библиотечная система IPRbooks [Электронный ресурс]. URL: <http://www.iprbookshop.ru/>

Электронная библиотека ВШТЭ СПб ГУПТД [Электронный ресурс]. URL: <http://nizrp.narod.ru>

Электронно-библиотечная система «Айбукс» [Электронный ресурс]. URL: <https://www.ibooks.ru/>

Информационная система «Единое окно доступа к образовательным ресурсам. Раздел. Информатика и информационные технологии» [Электронный ресурс].

7.3 Перечень лицензионного и свободно распространяемого программного обеспечения

Microsoft: WIN HOME 10 Russian OLP NL AcademicEdition Legalization GetGenuine

Microsoft: Office Standard 2016 Russian OLP NL AcademicEdition

7.4 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудитория	Оснащение
Лекционная аудитория	Мультимедийное оборудование, специализированная мебель, доска
Компьютерный класс	Мультимедийное оборудование, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду