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

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 7d15b88066d31dcb1847af0d7d99b718672f8b21
Владелец: Луканин Павел Владимирович
Действителен: с 11.02.2020 по 31.12.2022

Рабочая программа дисциплины

Б1.В.ДВ.01.02 Информационная безопасность

Учебный план: ФГОС3++z130301-3_22-15.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: заочная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия				
3	УП	4	4	60	4	2	Зачет
	РПД	4	4	60	4	2	
Итого	УП	4	4	60	4	2	
	РПД	4	4	60	4	2	

Санкт-Петербург
2022

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

Составитель (и):

старший преподаватель	Маслобоев А.Н.
От кафедры составителя: Заведующий кафедрой прикладной математики и информатики	Яковлев В.П.
От выпускающей кафедры: Заведующий кафедрой	Смородин С.Н.
Методический отдел:	Смирнова В.Г.

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: Цель изучения данной дисциплины — ознакомление с организационными, техническими, и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области,изучение методов защиты информации.

1.2 Задачи дисциплины:

Задачей изучения дисциплины является усвоение студентами основ информационной безопасности — источников, рисков и форм атак на информацию . Учащиеся должны уметь определять вредоносные программы и компьютерные вирусы. В процессе изучения предмета они приобретают знания в области правовых основ, политики и стандартов информационной безопасности. Происходит их знакомство с криптографическими моделями, алгоритмами шифрования, а с также антивирусной защитой и требованиями к системам информационной защиты ИС.

1.3 Требования к предварительной подготовке обучающегося:

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

Информатика

Информационные технологии

Информатика в задачах теплоэнергетики

Основы системного анализа

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 РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Инновац. формы занятий
		Лек. (часы)	Пр. (часы)		
Раздел 1. Введение в информационную безопасность	3				
Тема 1. Основные понятия и определения Модели информационной безопасности. Виды защищаемой информации. Обзор источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС		1	1	15	ИЛ
Тема 2. Правовые основы информационной безопасности. Основные нормативно-правовые акты в области информационной безопасности. Защита конфиденциальной информации. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС		1	1	15	
Раздел 2. Защита информации в компьютерных сетях					
Тема 3. Базовые понятия защиты информации в компьютерных сетях. Методы идентификации и проверки подлинности пользователей компьютерных систем. Основные этапы допуска к ресурсам компьютерной системы. Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet. Настройка и использование файрволов.		1	1	15	ИЛ
Тема 4. Антивирусная защита. Классификация компьютерных вирусов. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Разработка и основные принципы использования антивирусного программного обеспечения.		1	1	15	
Итого в семестре (на курсе для ЗАО)		4	4	60	

Консультации и промежуточная аттестация (Зачет)		0,25		
Всего контактная работа и СР по дисциплине		8,25	60	

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1 Описание показателей, критериев и системы оценивания результатов обучения

5.1.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения	Наименование оценочного средства
ПК-5.1	Имеет базовые знания об использовании современных средств защиты информации Демонстрирует навыки применения современных антивирусных средств и методов криптографии для защиты информации Свободно ориентируется в современной терминологии в области информационной безопасности	Вопросы устного собеседования. Практико-ориентированные задания.

5.1.2 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 объёме, 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.	

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

5.2.1 Перечень контрольных вопросов

№ п/п	Формулировки вопросов
	Курс 3
1	Защита от компьютерных вирусов.
2	Популярные антивирусные программы и их классификация.
3	Организация системы защиты информации экономических объектов.
4	Криптографические методы защиты информации.
5	Этапы построения системы защиты информации.
6	Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
7	Основные понятия информационной безопасности.

8	Система защиты информации и ее структура
9	Информация как товар и объект безопасности.
10	Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
11	Персональные данные и их защита.
12	Информационные угрозы, их виды и причины возникновения.
13	Способы воздействия информационных угроз на объекты.
14	Внешние и внутренние субъекты информационных угроз.
15	Вредоносные программы, их виды.
16	История компьютерных вирусов и современность.
17	Политика безопасности и ее принципы.
18	Фрагментарный и системный подход к защите информации
19	Методы и средства защиты информации.
20	Организационное обеспечение информационной безопасности
21	Организация конфиденциального делопроизводства.
22	Комплекс организационно-технических мероприятий по обеспечению защиты информации.
23	Инженерно-техническое обеспечение компьютерной безопасности.
24	Защита информации в Интернете

5.2.2 Типовые тестовые задания

Не предусмотрено

5.2.3 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

5.3 Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности)

5.3.1 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»

5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная	+	Письменная		Компьютерное тестирование		Иная	

5.3.3 Особенности проведения промежуточной аттестации по дисциплине

Время на подготовку к ответу по билету - 15 минут.
В течение семестра выполняются контрольные работы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Фомин, Д. В.	Информационная безопасность	Саратов, Москва: Профобразование, Ай Пи Ар Медиа	2022	https://www.iprbookshop.ru/118458.html
Куликов, С. С.	Информационная безопасность локальных компьютерных сетей	Воронеж: Воронежский государственный технический университет, ЭБС АСВ	2021	https://www.iprbookshop.ru/118614.html
сост., Кирколуп, Скурыдина, Е. М.	Информационная безопасность	Барнаул: Алтайский государственный педагогический университет	2017	http://www.iprbookshop.ru/102889.html

Куликов, С. С.	Информационная безопасность глобальных компьютерных сетей	Воронеж: Воронежский государственный технический университет, ЭБС АСВ	2021	https://www.iprbookshop.ru/118613.html
6.1.2 Дополнительная учебная литература				
Штеренберг, С. И.	Информационная безопасность. Стеганография	Санкт-Петербург: Санкт-Петербургский государственный университет промышленных технологий и дизайна	2017	http://www.iprbookshop.ru/102424.html
Ревнивых, А. В.	Информационная безопасность в организациях	Москва: Ай Пи Ар Медиа	2021	https://www.iprbookshop.ru/108227.html

6.2 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].

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftWindows 8

MicrosoftOfficeProfessional 2013

6.4 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