

УТВЕРЖДАЮ
Директор ВШТЭ



Рабочая программа дисциплины

Б1.В.ДВ.01.02 Информационная безопасность

Учебный план: ФГОС3++b130301-1_19-14.plx

Кафедра: **16** Прикладной математики и информатики

Направление подготовки:
(специальность) 13.03.01 Теплоэнергетика и теплотехника

Профиль подготовки: Промышленная теплоэнергетика
(специализация)

Уровень образования: бакалавриат

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоёмкость, 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 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

Сморodin 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 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:

Учебная практика (профилирующая практика)

Информатика в задачах теплоэнергетики

Информационные технологии

Правоведение

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПКп-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	Форма текущего контроля
		Лек. (часы)	Пр. (часы)			
Раздел 1. Введение в информационную безопасность	5					О
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		2	2	6	ИЛ	
Тема 2. Правовые основы информационной безопасности.						О
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		3	2	6		
Раздел 2. Шифрование данных						
Тема 3. Основы криптографии						О
Криптографические модели. Симметричные и асимметричные криптосистемы для защиты компьютерной информации в ИС. Цифровые (электронные) подписи. Инфраструктура открытых ключей. Криптографические протоколы.		4	2	6	ИЛ	
Тема 4. Стандартные алгоритмы шифрования.						
Безопасность и быстроедействие криптосистем. Зашифровывание и расшифровывание. Криптостойкость шифра. Абсолютно стойкие системы. Достаточно стойкие системы. Симметричное и асимметричное шифрование. Схемы их реализации. Управление ключами.		2	2	4		
Тема 5. Разработка программного обеспечения по шифрованию данных в среде объектно-ориентированного программирования.						О
Шифр Цезаря как частный случай шифра подстановки. Шифр Атбаш. Шифр Виженера. Одноразовый блокнот. Шифр перестановки. Шифр маршрутной перестановки. Шифр двойной перестановки.		2	3	7,75		
Раздел 3. Защита информации в компьютерных сетях						О

Тема 6. 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 <u>использование файрволов</u> .		2	2	4	ИЛ	
Тема 7. 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.		2	4	4		
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. 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
ПКп-5.1	Излагает базовые теоретические положения в области защиты информации и информационной безопасности Имеет представление об использовании современных средств криптографии для защиты информации Демонстрирует навыки применения современных антивирусных средств для защиты информации	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 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.	
--	---	--

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
Семестр 5	
1	Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2	Основные понятия информационной безопасности.
3	Система защиты информации и ее структура
4	Информация как товар и объект безопасности.
5	Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6	Персональные данные и их защита.
7	Информационные угрозы, их виды и причины возникновения.
8	Способы воздействия информационных угроз на объекты.
9	Внешние и внутренние субъекты информационных угроз.
10	Вредоносные программы, их виды.
11	История компьютерных вирусов и современность.
12	Политика безопасности и ее принципы.
13	Фрагментарный и системный подход к защите информации
14	Методы и средства защиты информации.
15	Организационное обеспечение информационной безопасности
16	Организация конфиденциального делопроизводства.
17	Комплекс организационно-технических мероприятий по обеспечению защиты информации.
18	Инженерно-техническое обеспечение компьютерной безопасности.
19	Защита информации в Интернете
20	Защита от компьютерных вирусов.
21	Популярные антивирусные программы и их классификация.
22	Организация системы защиты информации экономических объектов.
23	Криптографические методы защиты информации.
24	Этапы построения системы защиты информации.

5.2.2 Типовые тестовые задания

Не предусмотрены

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

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

2. Разработать в современной среде объектно-ориентированного программирования приложение

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 - 30 минут

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 и защита информации: специализированные аттестованные программные и программно-аппаратные средства	Саратов: Вузовское образование	2018	http://www.iprbookshop.ru/77317.html
Прохорова О. В.	Информационная безопасность и защита информации	Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ	2014	http://www.iprbookshop.ru/43183.html
6.1.2 Дополнительная учебная литература				
Горев А. И., Симаков А. А.	Обработка и защита информации в компьютерных системах	Омск: Омская академия МВД России	2016	http://www.iprbookshop.ru/72856.html
Никифоров С. Н.	Защита информации	Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ	2015	http://www.iprbookshop.ru/74365.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

1. Электронно-библиотечная система IPRbooks [Электронный ресурс]. URL: <http://www.iprbookshop.ru/>
2. Электронная библиотека ВШТЭ СПб ГУПТД [Электронный ресурс]. URL: <http://nizrp.narod.ru>

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftWindows 8
MicrosoftOfficeProfessional 2013
Delphi

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