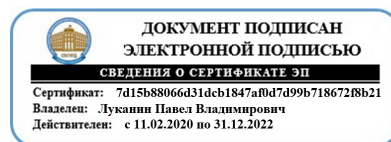


УТВЕРЖДАЮ
Директор ВШТЭ



Рабочая программа дисциплины

Б1.О.37 Информационная безопасность

Учебный план: ФГОС3++b010302-1_19-14.plx

Кафедра: **16** Прикладной математики и информатики

Направление подготовки:
(специальность) 01.03.02 Прикладная математика и информатика

Профиль подготовки: Прикладная математика и информатика
(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				
8	УП	18	54	36	36	4	Экзамен
	РПД	18	54	36	36	4	
Итого	УП	18	54	36	36	4	
	РПД	18	54	36	36	4	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 01.03.02 Прикладная математика и информатика, утверждённым приказом Министерства образования и науки Российской Федерации от 10.01.2018 г. № 9

Составитель (и):

старший преподаватель

Маслобоев А.Н.

От кафедры составителя:

Заведующий кафедрой прикладной математики и информатики

Яковлев В.П.

От выпускающей кафедры:

Заведующий кафедрой

Яковлев В.П.

Методический отдел:

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:

Web-страницы

Информатика

Языки и методы программирования

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-4: Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Знать: Принципы, методы и средства решения задач профессиональной деятельности с учетом основных требований информационной безопасности.

Уметь: Решать задачи профессиональной деятельности с учетом основных требований информационной безопасности.

Владеть: Навыками использования информационно-коммуникационных технологий с учетом основных требований информационной безопасности при решении задач профессиональной деятельности.
--

ОПК-1: Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности

Знать: Базовые теоретические положения в области информационной безопасности

Уметь: Использовать базовые теоретические положения дисциплины «Информационная безопасность» в профессиональной деятельности

Владеть: Навыками выбора методов решения задач профессиональной деятельности на основе теоретических знаний 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. Основные понятия и определения	8					О
Тема 1. Изучение источников, рисков и форм атак на информацию в ИС, вредоносных программ и компьютерных вирусов. Проблемы защиты информации в ИС		2	6	6	ИЛ	
Тема 2. Законодательные и правовые основы защиты компьютерной информации информационных технологий. Политика информационной безопасности. Содержание основных документов предприятия по обеспечению защиты компьютерной информации в ИС		4	4	6		
Раздел 2. Шифрование данных						О
Тема 3. Основы криптографии						
Криптографические модели. Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в ИС		4	8	6	ИЛ	
Тема 4. Стандартные алгоритмы шифрования. Безопасность и быстродействие криптосистем		2	6	4		
Тема 5. Разработка программного обеспечения по шифрованию данных в среде объектно-ориентированного программирования		2	10	6		
Раздел 3. Защита информации в компьютерных сетях						О
Тема 6. Методы идентификации и проверки подлинности пользователей компьютерных систем. Многоуровневая защита корпоративных сетей. Защита компьютерных систем от удаленных атак через сеть Internet		2	10	4	ИЛ	
Тема 7. Защита информации в компьютерных сетях, антивирусная защита. Разработка антивирусного программного обеспечения		2	10	4		
Итого в семестре (на курсе для ЗАО)		18	54	36		
Консультации и промежуточная аттестация (Экзамен)		2,5		33,5		
Всего контактная работа и СР по дисциплине		74,5		69,5		

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
ОПК-4	Излагает базовые теоретические положения в области защиты информации и информационной безопасности Имеет представление об использовании современных средств защиты информации Демонстрирует навыки применения современных антивирусных средств для защиты информации	Вопросы устного собеседования Практико-ориентированные задания
ОПК-1	Излагает базовые теоретические положения в области современных методов криптографии Имеет представление об использовании современных средств программирования для создания программ шифрования данных Демонстрирует навыки применения современных средств программирования для разработки приложений, осуществляющих шифрование данных	Вопросы устного собеседования Практико-ориентированные задания

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Обучающийся показывает всестороннее и глубокое знание теоретических основ дисциплины, свободно ориентируется в основных понятиях, терминах и определениях при ответе; знаком с дополнительной литературой; способен проработать научно-исследовательскую литературу по темам дисциплины и грамотно изложить материал. Качество исполнения всех элементов практического задания полностью соответствует предъявляемым требованиям.	
4 (хорошо)	Обучающийся показывает знание теоретических основ дисциплины, свободно ориентируется в основных понятиях, терминах и определениях при ответе; знаком с дополнительной литературой; способен проработать научно-исследовательскую литературу по темам дисциплины и грамотно изложить материал, но допускает ошибки при ответах на дополнительные вопросы преподавателя. Практическое задание выполнено в соответствии с поставленной задачей. Имеются отдельные несущественные ошибки или отступления от правил оформления.	
3 (удовлетворительно)	Обучающийся показывает неполное знание теоретических основ дисциплины, ориентируется в основных понятиях, терминах и определениях при ответе; не знаком с дополнительной литературой; может проработать научно-исследовательскую литературу по темам дисциплины, но не может грамотно и четко изложить материал, допускает ошибки при ответах на	

	дополнительные вопросы преподавателя. Практическое задание выполнено полностью, но с существенными ошибками. При этом нарушены правила оформления.	
2 (неудовлетворительно)	Обучающийся не знает теоретических основ дисциплины, способен проработать научно-исследовательскую литературу по темам дисциплины, но не может грамотно и четко изложить материал, допускает ошибки при ответах на дополнительные вопросы преподавателя. Отсутствие одного или нескольких обязательных элементов практического задания, либо грубые ошибки в работе.	

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 8	
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				
Башлы П. Н., Бабаши А. В., Баранова Е. К.	Информационная безопасность и защита информации	Москва: Евразийский открытый институт	2012	http://www.iprbookshop.ru/10677.html
Прохорова О. В.	Информационная безопасность и защита информации	Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ	2014	http://www.iprbookshop.ru/43183.html
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
6.1.2 Дополнительная учебная литература				
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://nizpr.narod.ru>

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

Microsoft Windows 8
Microsoft Office Professional 2013
Delphi
PTC Mathcad 15

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
--------------------	---