

Министерство образования и науки Российской Федерации

федеральное государственное бюджетное образовательное учреждение высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
ВЫСШАЯ ШКОЛА ТЕХНОЛОГИИ И ЭНЕРГЕТИКИ

УТВЕРЖДАЮ
 Директор ВШТЭ

 П.В.Луканин
 « 07 / 07 » 20 16 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.6.2
 (индекс дисциплины)

Информационная безопасность
 (Наименование дисциплины)

Кафедра: **16** Прикладной математики и информатики
 Код (Наименование кафедры)

Направление подготовки: **13.03.01** Теплоэнергетика и теплотехника

Профиль подготовки: **Промышленная теплоэнергетика**

Уровень образования: **Прикладной бакалавриат**

План учебного процесса

Составляющие учебного процесса		Очное обучение	Очно-заочное обучение	Заочное обучение
Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы)	Всего	72		
	Аудиторные занятия	33		
	Лекции	11		
	Лабораторные занятия			
	Практические занятия	22		
	Самостоятельная работа	39		
	Промежуточная аттестация			
Формы контроля по семестрам (номер семестра)	Экзамен			
	Зачет	6		
Общая трудоемкость дисциплины (зачетные единицы)		2		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам									
	1	2	3	4	5	6	7	8	9	10
Очная						2				
Очно-заочная										
Заочная										

1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1: Базовая Обязательная Дополнительно является факультативом
Вариативная По выбору

1.2. Цель дисциплины

Ознакомление студентов с основными направлениями деятельности по обеспечению информационной безопасности и защите информации, рассмотрение аспектов нормативно-правовой базы, регламентирующей данную деятельность, задач руководителей, специалистов по сохранности информационных ресурсов, средств и механизмов, в том числе аппаратно-программных, используемых для этих целей и методов их применения.

1.3. Задачи дисциплины

- сформировать общее представление об информационной безопасности, как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
- передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
- привить навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

1.4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Этап формирования
ОПК- 1	способностью осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий	2

Планируемые результаты обучения

Знать:

- 1) основные факты, базовые концепции, принципы, модели и методы в области информационных технологий;
- 2) технологию работы на ПК в современных информационных средах.

Уметь:

- 1) работать в сети Интернет;
- 2) решать задачи обработки данных с помощью современных инструментальных средств конечного пользователя.

Владеть:

- 1) современными информационными технологиями для решения общенаучных задач в своей предметной области и для организации своего труда (офисное ПО, математические и графические пакеты).

1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:

Информационные технологии (ОПК-1);
Топливо и теория горения (ОПК-1);
Техническая термодинамика (ОПК-1);
Гидрогазодинамика ч.1 Гидравлика (ОПК-1);
Гидрогазодинамика ч.2 Газодинамика (ОПК-1).

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Общие вопросы информационной безопасности			
Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности	18		
Основные понятия информационной безопасности (ИБ). Понятие тайны как объекта защиты ИБ. Организация защиты информации (ЗИ). Политика ИБ. Субъекты и средства, представляющие угрозу для ИБ. Субъекты и средства, осуществляющие защиту информации.			
Тема 2. Защита информации в информационных системах	16		
Основные принципы организации процесса защиты информации. Угрозы информационной безопасности. Средства защиты информации. Защита информации от утечки по техническим каналам. Оценка эффективности системы ИБ. Средства несанкционированного доступа и защиты аудио информации. Средства несанкционированного доступа и защиты видео информации.			
Текущий контроль 1 (тестирование)	2		
Учебный модуль 2. Нормативно-правовые вопросы защиты информации			
Тема 3. Нормативно-правовые аспекты информационной безопасности и защиты информации	14		
Основы нормативно-правовой защиты информации (ЗИ). Основные нормативные документы РФ по ЗИ. Защита государственной тайны. Защита коммерческой тайны (КТ). Доктрина ИБ РФ. Государственные органы РФ, отвечающие за нормативно-правовое обеспечение ИБ.			
Тема 4. Административно-организационные аспекты информационной безопасности и защиты информации	12		
Организационная защита информации. Работа с конфиденциальной информацией. Функции службы безопасности. Классификация способов защиты информации. Основные действия по защите информации. Процессы создания и эксплуатации системы информационной безопасности. Типовая модель многорубежной системы защиты информации.			
Текущий контроль 2(тестирование)	2		
Промежуточная аттестация по дисциплине (Зачет)	8		
	72		

3. ТЕМАТИЧЕСКИЙ ПЛАН

3.1. Лекции

Номера изучаемых тем	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	6	3				
2	6	3				
3	6	3				
4	6	2				
ВСЕГО:		11				

3.2. Практические занятия

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	Национальная безопасность Российской Федерации: решение задач	6	4				
2	Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере Основные понятия и общеметодологические принципы теории информационной безопасности: решения задач	6	6				
3	Понятие и виды защищаемой информации (ПЗ) Понятие и виды угроз информационной безопасности (ПЗ) Информационная безопасность и информационное противоборство: решение задач	6	6				
4	Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны Методы и средства обеспечения информационной безопасности компьютерных систем: решение задач	6	6				
ВСЕГО:			22				

3.3. Лабораторные занятия

Не предусмотрено.

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Не предусмотрено.

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

Номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1,2	Тестирование	6	2				

6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
Усвоение теоретического материала	6	17				
Подготовка к практическим занятиям	6	14				
Подготовка к зачету	6	8				
ВСЕГО:		39				

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий
Не предусмотрено.

7.2. Система оценивания успеваемости и достижений обучающихся для промежуточной аттестации

традиционная

балльно-рейтинговая

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с Режим доступа: IPRbooks - <http://www.iprbookshop.ru/52209>
2. Нестеров С.А. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Нестеров С.А.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014.— 322 IPRbooks - <http://www.iprbookshop.ru/43960>

б) дополнительная учебная литература

3. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИБ), 2014.— 256 c IPRbooks -<http://www.iprbookshop.ru/33430>
4. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс]/ Шаньгин В.Ф.— Электрон. текстовые данные.— М.: ДМК Пресс, 2014.— 702 c IPRbooks - <http://www.iprbookshop.ru/29257>

8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара: Самарский государственный архитектурно-строительный университет, 2014
2. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. - 253 с.

8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1. Образовательный математический сайт "Exponenta.ru" <http://www.exponenta.ru/>
2. Виртуальный музей Информатики <http://informat444.narod.ru/museum/>
3. Сайта министерства информатизации www.informika.ru

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Microsoft Windows 8.1
2. Microsoft Office Professional 2013

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

Компьютерный класс с персональными компьютерами на базе процессоров не ниже IntelPentium 4, с оперативной памятью не ниже 2 Гб.

8.6. Иные сведения и (или) материалы

Не предусмотрено.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Лекции	<p>Лекции обеспечивают теоретическое изучение дисциплины. На них излагается основное содержание курса, иллюстрируемое конкретными примерами, широко используется зарубежный и отечественный опыт использования систем информационной безопасности.</p> <p>Освоение лекционного материала обучающимся предполагает следующие виды работ:</p> <ul style="list-style-type: none"> • конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы и формулировки; пометать важные мысли, выделять ключевые слова, термины. • проверка терминов, понятий: осуществлять с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь; • работа с теоретическим материалом (конспектирование источников): найти ответ на вопросы в рекомендуемой литературе. <p>Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на практическом занятии.</p>
Практические занятия	<p>На практических занятиях разъясняются теоретические положения курса, студенты выполняют задания, практически иллюстрирующие лекционный материал, овладевают навыками сбора, анализа и обработки информации для принятия самостоятельных решений, навыками работы с системами информационной безопасности.</p> <p>Подготовка к практическим занятиям предполагает следующие виды работ:</p> <ul style="list-style-type: none"> • работа с конспектом лекций; • подготовка ответов к контрольным вопросам, тестовым заданиям; • просмотр рекомендуемой литературы, работа с текстом (указать текст из источника и др.); • подготовка и сдача отчетов по выполненным практическим работам.
Самостоятельная работа	<p>При подготовке к зачету необходимо ознакомиться с демонстрационным вариантом задания (теста, перечнем вопросов), проработать конспекты лекций и практических занятий, рекомендуемую литературу, получить консультацию у преподавателя, подготовить презентацию материалов.</p>

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

10.1.1. Показатели оценивания компетенций на этапах их формирования

Код компетенции (этап освоения)	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ОПК-1 (2)	1. Излагает базовые законы информатики и имеет представление об основных информационных процессах 2. Демонстрирует применение базовых законов и принципов информатики к решению задач 3. Использует теоретические знания по информатике для решения практических задач	1. Устное собеседование 2. Практическое задание	1. Перечень вопросов к зачету (17 вопросов) 2. Практические задания (20 заданий)

10.1.2. Описание шкал и критериев оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

Оценка по традиционной шкале	Критерии оценивания сформированности компетенций
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 практических задач, владеет необходимыми навыками и приемами их выполнения.
Не зачтено	Обучающийся не может изложить значительной части программного материала, допускает существенные ошибки, допускает неточности в формулировках и доказательствах, нарушения в последовательности изложения программного материала; неуверенно, с большими затруднениями выполняет практические задания.

10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

10.2.1. Перечень вопросов к зачету, разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировки вопросов	№ темы
1	Понятие национальной безопасности Российской Федерации.	1
2	Национальные интересы РФ и стратегические национальные приоритеты.	1
3	Роль информационной безопасности в обеспечении национальной безопасности государства	1
4	Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере	2
5	Основные понятия и общеметодологические принципы теории информационной безопасности	2
6	Основные составляющие национальных интересов Российской Федерации в информационной сфере	2
7	Понятие информационной безопасности Российской Федерации.	2
8	Интересы личности общества и государства в информационной сфере.	3
9	Виды угроз информационной безопасности Российской Федерации.	4
10	Понятие и виды защищаемой информации	3
11	Понятие и виды угроз информационной безопасности	3

12	Информационная безопасность и информационное противоборство	3
13	Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны	4
14	Методы и средства обеспечения информационной безопасности компьютерных систем	4
15	Внешние и внутренние источники угроз информационной безопасности Российской Федерации.	4
16	Методы обеспечения информационной безопасности Российской Федерации	4
17	Источники понятий в области информационной безопасности.	4

10.2.2 Перечень типовых заданий, разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Условия заданий	Ответ																																																				
1	Необходимо зашифровать сообщение по методу Цезаря. Исходное сообщение: «Криптография»; ключ 3	<table border="1"> <tr> <td>Сообщение</td> <td>К</td> <td>Р</td> <td>И</td> <td>П</td> <td>Т</td> <td>О</td> <td>Г</td> <td>Р</td> <td>А</td> <td>Ф</td> <td>И</td> <td>Я</td> </tr> <tr> <td>Номер 1</td> <td>12</td> <td>18</td> <td>10</td> <td>17</td> <td>20</td> <td>16</td> <td>4</td> <td>18</td> <td>1</td> <td>22</td> <td>10</td> <td>33</td> </tr> <tr> <td>Номер 1 + 3</td> <td>15</td> <td>21</td> <td>13</td> <td>20</td> <td>23</td> <td>19</td> <td>7</td> <td>21</td> <td>4</td> <td>25</td> <td>13</td> <td>3</td> </tr> <tr> <td>Шифр</td> <td>Н</td> <td>У</td> <td>Л</td> <td>Т</td> <td>Х</td> <td>С</td> <td>Е</td> <td>У</td> <td>Г</td> <td>Ч</td> <td>Л</td> <td>В</td> </tr> </table> <p>Номер 1 – номер буквы согласно табл. Номер 1 + 3 – номер буквы согласно табл. + ключ (перемещаем букву на 3 позиции вперед) Шифр: «НУЛТХСЕУГЧЛВ» Ответ: «НУЛТХСЕУГЧЛВ»</p>	Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я	Номер 1	12	18	10	17	20	16	4	18	1	22	10	33	Номер 1 + 3	15	21	13	20	23	19	7	21	4	25	13	3	Шифр	Н	У	Л	Т	Х	С	Е	У	Г	Ч	Л	В
Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я																																										
Номер 1	12	18	10	17	20	16	4	18	1	22	10	33																																										
Номер 1 + 3	15	21	13	20	23	19	7	21	4	25	13	3																																										
Шифр	Н	У	Л	Т	Х	С	Е	У	Г	Ч	Л	В																																										
2	Необходимо зашифровать текст с помощью шифра Атбаш. Исходное слово: «замена»	Шифрование осуществляется путем замены первой буквы алфавита на последнюю, второй на предпоследнюю и так далее. Зашифрованное слово: «чяться»																																																				
3	Необходимо зашифровать текст с помощью шифра Гронсфельда. Исходное словосочетание: «шифр гронсфельда»; ключ 15382	Зашифрованный текст: «щнчшесурьцёрялв»																																																				

10.3. Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

10.3.1. Условия допуска обучающегося к сдаче зачета и порядок ликвидации академической задолженности

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся (принято на Ученом совете университета 15.03.2016г., протокол № 4)

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная письменная компьютерное тестирование иная*

10.3.3. Особенности проведения зачета:

- Возможность пользоваться справочными таблицами, калькулятором;
- Время на подготовку ответа 20 минут;
- Зачет проводится в компьютерном классе.