Министерство науки и высшего образования 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

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 — **Информационная безопасность теплотехнологических объектов**

(индекс дисциплины) *(Наименование дисциплины)*

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

Направление подготовки: 13.03.01 Теплоэнергетика и теплотехника

Профиль подготовки: Энергетика теплотехнологий

Уровень образования : 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	**144**		
	Аудиторные занятия	**72**		
	Лекции	18		
	Практические занятия	54		
	Самостоятельная работа	**72**		
	Промежуточная аттестация			
Формы контроля по семестрам (номер семестра)	Экзамен			
	Зачет	5		
Общая трудоемкость дисциплины (зачетные единицы)		**4**		

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

Санкт-Петербург
2020

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 13.03.01 Теплоэнергетика и теплотехника

На основании учебных планов № b130301-3_20

Кафедра-разработчик: Прикладной математики и информатики

Заведующий кафедрой: Яковлев В.П.

СОГЛАСОВАНИЕ:

Выпускающая кафедра: Промышленной теплоэнергетики

Заведующий кафедрой: Смородин С.Н.

Методический отдел: Смирнова В.Г.

1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1:	Базовая		Обязательная		Дополнительно является факультативом
	Вариативная	x	По выбору	x	

1.2. Цель дисциплины

Сформировать компетенции обучающегося в области освоения базовых технологий обеспечения информационной безопасности теплоэнергетических объектов.

1.3. Задачи дисциплины

- изучить основные положения, понятия и категории, относящиеся к базовым технологиям обеспечения информационной безопасности;
- изучить требования, предъявляемых к процессам защиты информации в современных информационных системах;
- освоить типовые подходы и методы противодействия наиболее распространенным угрозам информационной безопасности;
- овладеть принципами организации, комплексного подхода к выбору средств и технологий обеспечения информационной безопасности теплоэнергетических объектов.

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 понятия из области информационной безопасности; 2) классификацию угроз информационной безопасности объектов. Уметь: 1) использовать интернет-ресурсы и поисковые системы для получения необходимой информации из области информационной безопасности; 2) применять современное программное обеспечение для анализа и обработки полученной информации. Владеть: 1) навыками использования современных информационных технологий в сфере информационной безопасности; 2) приемами противодействия угрозам информационной безопасности объектов.		
ПК-2	способностью проводить расчеты по типовым методикам, проектировать технологическое оборудование с использованием стандартных средств автоматизации проектирования в соответствии с техническим заданием	1
Знать: 1) основные способы противодействия угрозам из области информационной безопасности; 2) отечественные и международные стандарты в области обеспечения информационной безопасности. Уметь:		

Код компетенции	Формулировка компетенции	Этап формирования
1) установить программное обеспечение, необходимое для обеспечения информационной безопасности объекта; 2) использовать имеющуюся информацию для выработки стратегии защиты объектов от информационных угроз. Владеть: 1) методикой эффективной эксплуатации программного обеспечения применяемого для обеспечения информационной безопасности; 2) современными криптографическими технологиями защиты информации.		

1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:
Информатика в задачах теплоэнергетики и теплотехнологии (ОПК-1, ПК-2)
Техническая термодинамика (ПК-2)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Информационно-аналитическая деятельность в сфере безопасности			
Тема 1. Концептуальные основы защиты информации	16		
Введение в дисциплину. Система документов по технической защите информации. Законодательные и иные правовые акты в области технической защиты информации. Государственные органы по технической защите информации в РФ. Лицензирование деятельности в области защиты информации.			
Тема 2. Классификация угроз и объектов защиты	19		
Методы оценки опасности угроз. Объект информатизации. Классификация объектов защиты. Угрозы несанкционированного доступа к информации. Основные классы атак в сетях. Понятие несанкционированного доступа. Межсетевой экран. Система обнаружения вторжений			
Текущий контроль 1 (устный опрос).	1		
Учебный модуль 2. Базовые требования по защите информации			
Тема 3. Основные рекомендации по защите информации	20		
Порядок обеспечения защиты информации. Защита конфиденциальной информации на автоматизированных рабочих местах. Защита информации в локальных вычислительных сетях. Защита информации при межсетевом взаимодействии. Защита информации при работе с системами управления базами данных. Порядок обеспечения защиты информации при взаимодействии с информационными сетями общего пользования. Основные требования и рекомендации по защите служебной тайны и персональных данных.			
Тема 4. Технические каналы утечки информации	15		
Понятие информационного сигнала. Модуляция сигналов. Опасные сигналы и их источники. Основные показатели технического канала утечки информации			
Текущий контроль 2 (устный опрос).	1		
Учебный модуль 3. Компьютерные вирусы и защита от них			
Тема 5. Вирусы как угроза информационной безопасности.	17		
Характерные черты компьютерных вирусов. Классификация компьютерных вирусов по среде обитания, по особенностям алгоритма работы, по			

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
деструктивным возможностям. Вирусоподобные программы. Утилиты скрытого администрирования.			
Тема 6. Антивирусные программы	18		
Особенности работы антивирусных программ. Классификация антивирусных программ. Факторы, определяющие качество антивирусных программ.			
Текущий контроль 3 (устный опрос)	1		
Учебный модуль 4. Механизмы обеспечения информационной безопасности			
Тема 7. Идентификация и аутентификация. Методы разграничения доступа	15		
Определение понятий «аутентфикация» и «идентификация». Механизм аутентификации и идентификации пользователей. Мандатное и дискретное управление доступом.			
Тема 8. Криптография и шифрование	16		
Структура криптосистемы. Классификация систем шифрования данных. Симметричные и ассимметричные методы шифрования. Механизм электронной цифровой подписи.			
Текущий контроль 4 (устный опрос).	1		
Промежуточная аттестация по дисциплине (зачет)	**4**		
ВСЕГО:	**144**		

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	5	2				
2	5	2				
3	5	2				
4	5	2				
5	5	2				
6	5	2				
7	5	2				
8	5	4				
ВСЕГО:		**18**				

3.2. Практические и семинарские 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	Анализ рисков информационной безопасности	5	6				
2	Основные принципы обеспечения информационной безопасности в России и ведущих зарубежных странах	5	6				
3	Построение концепции информационной безопасности объекта	5	6				
4	Построение VPN (виртуальной частной сети) на базе имеющегося программного обеспечения	5	6				
5	Алгоритмы поведения	5	6				

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)
	вирусных и других вредоносных программ						
6	Алгоритмы предупреждения и обнаружения вирусных угроз	5	6				
6	Пакеты антивирусных программ	5	4				
7	Процедура аутентификации пользователя на основе пароля.	5	4				
7	Механизмы контроля целостности данных	5	6				
8	Программная реализация криптографических алгоритмов	5	4				
		ВСЕГО:	**54**				

3.3. Лабораторные занятия
не предусмотрены.

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
1-4	Устный опрос	5	4				

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	5	20				
Подготовка к практическим занятиям	5	48				
Подготовка к зачету	5	4				
	ВСЕГО:	**72**				

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий:
не предусмотрены.

7.2. Система оценивания успеваемости и достижений обучающихся для промежуточной аттестации

традиционная [x] балльно-рейтинговая [ ]

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

1. Грошев, А.С. Информатика [Электрон. ресурс]: учебник для вузов / А.С. Грошев. – М.-Берлин.: Директ-Медиа, 2015.-484с. («КнигаФонд»: Режим доступа: http://www.knigafund.ru/183666/)
2. Ефремов, И.В. Информационные технологии в сфере безопасности [Электрон. ресурс]: практикум / И.В. Ефремов, В.А. Солопова – Оренбургский гос. ун-т. – Оренбург: ОГУ, 2013. - 116с. («КнигаФонд»: Режим доступа: http://www.knigafund.ru/181098/)

б) дополнительная учебная литература

3. Ачкасов В.Ю. Программирование на Lazarus [Электронный ресурс]: практикум/ В.Ю.Ачкасов— М.: Национальный открытый университет «Интуит», 2016.— 521 с.— («КнигаФонд»: Режим доступа: http://www.knigafund.ru/177930/)
4. Царев, Р.Ю. Программные и аппаратные средства информатики [Электрон. ресурс] / Р.Ю. Царев, А.В. Прокопенко, А.Н. Князьков - Красноярск: Сиб. федер. ун-т, 2015. - 160с. («КнигаФонд»: Режим доступа: http://www.knigafund.ru/182963/)

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

5. Информационная безопасность. [Электронный ресурс]: учебно-практическое пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К. — М.: Изд. центр ЕОАИ, 2011.— 376 с. («КнигаФонд»: Режим доступа: http://www.knigafund.ru/187025)

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

1. официальные сайты учреждений и организаций: комитет по информатизации и связи правительства Санкт-Петербурга [Электронный ресурс]. URL: http://kis.gov.spb.ru.

2. образовательные ресурсы: Информационная система «Единое окно доступа к образовательным ресурсам» [Электронный ресурс] . URL: http://window.edu.ru.

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

1. Microsoft Windows 8.1
2. Microsoft Office Professional 2013

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

1. компьютерный класс с мультимедийным комплексом;

8.6. Иные сведения и (или) материалы

не предусмотрены.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Лекции	Лекции обеспечивают теоретическое изучение дисциплины. На лекциях излагается основное содержание курса, иллюстрируемое конкретными примерами, широко используется зарубежный и отечественный опыт по тематике изучаемой дисциплины. Освоение лекционного материала обучающимися предполагает следующие виды работ: • проработка рабочей программы в соответствии с целями и задачами, структурой и содержанием дисциплины; • конспект лекций: кратко, схематично, последовательно фиксировать основные положения, выводы и формулировки; помечать важные мысли, выделять ключевые слова, термины; • проверка терминов, понятий: осуществлять с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь;

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
	• работа с теоретическим материалом (конспектирование источников): найти ответ на вопросы в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или на практическом занятии.
Практические занятия	На практических занятиях разъясняются теоретические положения курса, обучающиеся работают с конкретными ситуациями, овладевают навыками сбора, анализа и обработки информации для принятия самостоятельных решений, навыками подготовки информационных обзоров и аналитических отчетов по соответствующей тематике, навыками работы в малых группах. Подготовка к практическим занятиям предполагает следующие виды работ: • работа с конспектом лекций; • подготовка ответов к контрольным вопросам; • просмотр рекомендуемой литературы; • создание приложения по заданию преподавателя.
Самостоятельная работа	Данный вид работы предполагает расширение и закрепление знаний, умений и навыков, усвоенных на аудиторных занятиях путем самостоятельной проработки учебно-методических материалов по дисциплине и другим источникам информации; подготовки к зачету. Самостоятельная работа выполняется индивидуально, а также может проводиться под руководством преподавателя. При подготовке к зачету необходимо ознакомиться с перечнем вопросов к зачету, проработать конспекты лекций и практических занятий, рекомендуемую литературу, получить консультацию у преподавателя.

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 теоретические положения по дисциплине. Имеет представление об основных принципах работы современной вычислительной техники применительно к задачам информационной безопасности 2. Демонстрирует умение получать знания о современных методах применения информационных технологий в области информационной безопасности	1. Устное собеседование 2. Практическое типовое задание	1. Перечень вопросов к зачету (15 вопросов) 2. Практические типовые задания (8 задач)
ПК-2(1)	1. 1. Имеет представление об основах применения современных методов защиты информации 2. Демонстрирует умение применять изученные методы защиты информации для решения конкретных задач.	1. Устное собеседование 2. Практическое типовое задание	1. Перечень вопросов к зачету (15 вопросов) 2. Практические типовые задания (8 задач)

10.1.2. Описание шкал и критериев оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

Оценка по традиционной шкале	Критерии оценивания сформированности компетенций
Зачтено	Обучающийся: • ответил на поставленные вопросы; • выполнил практическое задание и представил результаты; возможно допуская несущественные ошибки.
Не зачтено	Обучающийся: • не выполнил практическое задание; • не ответил на вопросы преподавателя, или допустил существенные ошибки в ответе.

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	Формулировка вопросов	№ темы
1.	Составляющие информационной безопасности	1
2.	Доступность и целостность информации	1
3.	Конфиденциальность информации	1
4.	Основные задачи информационной безопасности общества	1
5.	Законодательно-правовой уровень формирования режима информационной безопасности	2
6.	Программно-технический уровень формирования режима информационной безопасности	2
7.	Административный уровень формирования режима информационной безопасности	2
8.	Основные категории государственных информационных ресурсов	2
9.	Критерии оценки безопасности информационных технологий	2
10.	Функциональные требования и требования доверия к информационным системам	2
11.	Основные механизмы обеспечения безопасности в вычислительных сетях.	3
12.	Администрирование средств безопасности.	3
13.	Взаимосвязь функций и механизмов безопасности	3
14.	Классы защищенности межсетевых экранов	3
15.	Классы угроз информационной безопасности	3
16.	Субъекты информационных отношений и их роли при обеспечении информационной безопасности	3
17.	Политика безопасности	4
18.	Каналы несанкционированного доступа к информации	4
19.	Упреждающая защита в информационных системах	4
20.	Характерные черты компьютерных вирусов	5
21.	Файловые и загрузочные вирусы	5
22.	Особенности резидентных вирусов.	5
23.	Стелс-вирусы.	5
24.	Самошифрование и полиморфичность как свойства компьютерных вирусов	5
25.	Основные виды антивирусных программ	6
26.	Особенности эвристических сканеров	6
27.	Симметричные алгоритмы шифрования	7

28.	Ассимметричные алгоритмы шифрования	7
29.	Цифровая подпись	8
30.	Открытые ключи шифрования	8

10.2.2 Вариант типовых заданий (задач), разработанных в соответствии с установленными этапами формирования компетенций

Типовое задание 1:
Разработать в Object Pascal приложение, представляющее собой форму доступа к определённым информационным ресурсам на основе пароля:
Ответ:

```
var
  myFile : TextFile;
  text   : string;

begin
  // Попытка открыть файл Test.txt для записи
  AssignFile(myFile, 'Test.txt');
  ReWrite(myFile);

  // Запись нескольких известных слов в этот файл
  WriteLn(myFile, 'Hello');
  WriteLn(myFile, 'World');

  // Закрытие файла
  CloseFile(myFile);

  // Открытие файла в режиме только для чтения
  FileMode := fmOpenRead;
  Reset(myFile);

  // Показ содержимого файла
  while not Eof(myFile) do
  begin
    ReadLn(myFile, text);
    ShowMessage(text);
  end;

  // Закрытие файла в последний раз
  CloseFile(myFile);
end;
end.
```

Типовое задание 2:

Составить на языке Object Pascal программу шифрования текста методом Льюиса.

Ответ:

```
const
  len = 26;

  //это символы для выбора столбца таблицы
  alpha_hor: string = 'abcdefghijklmnopqrstuvwxyz';
```

```
  //здесь будут символы для выбора строки таблицы
  alpha_ver: string = '';

var
  //это собственно таблица кодирования
  table: array[1 .. len, 1 .. len] of char;

function shift(s: string; n: integer): string;
  begin
  s := copy(s, length(s) - pred(n), n) + s;
  delete(s, length(s) - pred(n), n); shift := s
  end;

var
  i, j, row, col: integer;
  s: string; ch: char;

  key: string;
  is_russian: boolean;
  f_in: file of char; f_out, f_key: text;
begin
  // заполнение таблицы кодировки
  for i := 1 to len do
  begin
  //получаем строку символов для текущей строки таблицы
  s := shift(alpha_hor, pred(i));
  for j := 1 to len do
  table[i, j] := s[j];
  alpha_ver := alpha_ver + s[1]
  end;

  // связываем логические файлы программы с физическими файлами на диске

  //файл с фразой для кодирования - открываем для чтения
  assign(f_in, 'f_00in.txt');
  {$i-} reset(f_in); {$i+}

  //файл для сохранения результата - открываем для записи
  assign(f_out, 'f_00out.txt');
  {$i-} rewrite(f_out); {$i+}

  assign(f_key, 'f_00key.txt');
  {$i-} reset(f_key); {$i+}
  readln(f_key, key);
  close(f_key);

  //счетчик закодированных символов
  i := 0;
  //до конца кодируемого файла делаем следующее:
  while not eof(f_in) do
  begin
  //читаем очередной символ
```

```
read(f_in, ch);
//находим по нему строку таблицы
row := pos(ch, alpha_ver);

is_russian := (row > 0);
if is_russian then
begin
//если символ присутствует в таблице, его надо кодировать

//увеличиваем счетчик закодированных символов
inc(i);

  col := pos(key[i mod (length(key))], alpha_hor);
//и заменяем простой символ на зашифрованный (из таблицы)
ch := table[row, col];
end;
write(f_out, ch)
end;

// закрываем оба файла: исходный и зашифрованный
close(f_out);
close(f_in)
end.
```

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.

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная	X	письменная		компьютерное тестирование		иная*	

10.3.3. Особенности проведения зачета

- Возможность пользоваться справочным материалом;
- Время на подготовку ответа 30 минут.
- Зачет проводится в компьютерном классе.