Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
ФГБОУ ВО «КГТУ»
БГАРФ

УТВЕРЖДАЮ

И.О. декана РТФ

В.А. Баженов

27.06.2018 г.

Рабочая программа дисциплины
Теоретические основы компьютерной безопасности
(наименование дисциплины)
вариативной части образовательной программы
по специальности

10.05.03 Информационная безопасность автоматизированных систем
(код и наименование специальности)

«Обеспечение информационной безопасности распределенных информационных систем»
(наименование специализации)

Факультет/институт: Радиотехнический (РТФ)
(наименование)
Кафедра информационной безопасности
(наименование)

Калининград 2018 г.

1. Цель освоения дисциплины.

1.1. Цель изучения дисциплины:

- обучить студентов принципам и методам защиты информации;
- обучить студентов принципам комплексного проектирования, построения, обслуживания и анализа защищенных автоматизированных систем (АС);
- содействовать формированию научного мировоззрения и развитию системного мышления.

1.2. Задачи изучения дисциплины.

- дать основы:
- построения комплексов программно-аппаратных средств обеспечения информационной безопасности различной архитектуры;
- направлений обеспечения защиты ресурсов вычислительных сетей и СУБД от атак вредоносных программ и злоумышленников;
- принципов функционирования современных систем аудита ресурсов ВС;
- построения систем адаптивной безопасности в вычислительных сетях передачи данных;
- способов защиты трафика от изучения, разрушающих программных действий и изменений.

1.3 Предметом изучения дисциплины являются:

- сетевые атаки в автоматизированных системах, методы, способы и средства защиты от сетевых атак.

2. Результаты освоения дисциплины

Таблица 1 - Компетенции, формируемые в результате освоения дисциплины

Коды компетенций	Описание компетенций	Краткое содержание и структура компетенций.
ПК-6	способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	знать: методики анализа эффективного применения автоматизированных систем в сфере профессиональной деятельности уметь: предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности владеть: анализа эффективного применения автоматизированных систем в сфере профессиональной деятельности
ПК-11	способностью разрабатывать политику информационной безопасности автоматизированной системы	Знать: политику информационной безопасности автоматизированной системы Уметь: разрабатывать политику информационной безопасности автоматизированной системы Владеть: способностью разрабатывать политику информационной безопасности автоматизированной системы

ПК-13	способностью участвовать в проектировании средств защиты информации	знать: методы проектирования средств защиты информации уметь: разрабатывать и исследовать модели информационно-технологических ресурсов, проектировать средств защиты информации владеть: Методами исследования информационно-технологических ресурсов, методами проектирования средств защиты информации

Таблица 2 - Этапы формирования компетенций

Коды компетенций	Этапы формирования компетенций (разделы программы)
ПК-6 ПК-11 ПК-13	Тема 1. Введение. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ. Тема 2. Ценность информации. Тема 3.Анализ угроз информационной безопасности. Тема 4. Структура теории компьютерной безопасности. Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности информации. Тема 6. Построение систем защиты от угрозы нарушения целостности информации. Тема 7. Построение системы защиты от угрозы доступности информации. Построение системы защиты от угрозы раскрытия параметров информационной системы. Тема 8. Методология обследования и проектирования защиты АС. Тема 9. Понятие политики безопасности. Тема 10. Модели безопасности. Тема 11. Основные критерии оценки защищенности АС. Тема 12. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»). Тема 13. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ. Тема 14. Единые критерии безопасности информационных технологий (Common Criteria).

Таблица 3 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	- методологические и технологические основы комплексного обеспечения безопасности АС, - угрозы и методы нарушения безопасности АС, - формальные модели, лежащие в основе систем защиты АС, - стандарты по оценке защищенности АС и их теоретические основы, - методы и средства реализации защищенных АС, - методы и средства верификации и анализа надежности защищенных АС

уметь	- проводить анализ АС с точки зрения обеспечения компьютерной безопасности, - разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы, - применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС, - реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС
владеть	- навыками работы с АС распределенных вычислений и обработки информации; - навыками работы с документацией АС, - навыками использования критериев оценки защищенности АС, - навыками построения формальных моделей систем защиты информации АС

3. Место дисциплины в структуре образовательной программы

Место дисциплины в структуре ООП специалитета:
Б1.В.06. Теоретические основы компьютерной безопасности. Вариативная часть. Изучение дисциплины производится в тесной взаимосвязи с базовыми и вариативными математическими и естественнонаучными дисциплинами.

Требования к предварительной подготовке обучающегося:

«Алгебра и геометрия» - знать математический аппарат, основные алгебраические структуры и работу с ними.

«Математическая логика и теория алгоритмов» - знать математический аппарат, логические операции, алгебру предикатов, понятие машины Тьюринга, алгоритмической неразрешимости, сложности алгоритмов.

«Дискретная математика» знать приёмы работы с дискретными структурами, основы комбинаторики, теорию множеств, теорию графов и теорию конечных автоматов;

«Информатика» - знать формы и способы представления данных в персональном компьютере, классификацию современных компьютерных систем, типовые структуры и принципы организации компьютерных сетей; уметь применять типовые программные средства сервисного назначения (средства восстановления системы после сбоев, дефрагментации и очистки диска и т.п.), пользоваться сетевыми средствами и внешними носителями информации для обмена данными; владеть навыками обеспечения безопасности информации с помощью типовых программных средств (антивирусов, архиваторов, стандартных сетевых средств обмена информацией и т.п.), навыками поиска и обмена информацией в глобальной информационной сети Интернет;

«Основы информационной безопасности» - знать основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации; уметь классифицировать и оценивать угрозы информационной безопасности для объекта информатизации; владеть профессиональной терминологией в области информационной безопасности.

Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

«Разработка и эксплуатация защищенных автоматизированных систем», «Программно-аппаратные средства обеспечения информационной безопасности», "Комплексное обеспечение информационной безопасности автоматизированных систем".

4. Содержание дисциплины:

Тема 1. Введение. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ.
Тема 2. Ценность информации.
Тема 3.Анализ угроз информационной безопасности.
Тема 4. Структура теории компьютерной безопасности.
Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности информации.
Тема 6. Построение систем защиты от угрозы нарушения целостности информации.
Тема 7. Построение системы защиты от угрозы доступности информации. Построение системы защиты от угрозы раскрытия параметров информационной системы.
Тема 8. Методология обследования и проектирования защиты АС.
Тема 9. Понятие политики безопасности.
Тема 10. Модели безопасности.
Тема 11. Основные критерии оценки защищенности АС.
Тема 12. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).
Тема 13. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.
Тема 14. Единые критерии безопасности информационных технологий (Common Criteria).

5. Объем (трудоемкость освоения) и структура дисциплины, формы аттестации

Таблица 1 - Объем (трудоемкость освоения) и структура дисциплины, формы аттестации для очной формы обучения

Номер и наименование Разделов и тем	Объем учебной работы (час.)					
	Лек	ЛЗ	ПЗ	СРС	Котроль	Все-
Семестр - 7 (180 час; 5 ЗЕТ).						
Тема 1. Введение. Основные понятия теории компьютерной безопасности. Язык. Объекты. Субъекты. Доступ.	3			5		8
Тема 2. Ценность информации.	2					2
Тема 3.Анализ угроз информационной безопасности.	2			5		7
Тема 4. Структура теории компьютерной безопасности.	3	4				7
Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности информации.	2			5		7
Тема 6. Построение систем защиты от угрозы нарушения целостности информации.	2					2
Тема 7. Построение системы защиты от угрозы доступности информации. Построение системы защиты от угрозы раскрытия параметров информационной системы.	2	4		5		11
Тема 8. Методология обследования и проектирования защиты АС.	2	4	2			8
Тема 9. Понятие политики безопасности.	2			5		7
Тема 10. Модели безопасности.	6		28			34

Тема 11. Основные критерии оценки защищенности АС.	2			5		7
Тема 12. Стандарт оценки безопасности компьютерных систем TCSEC («Оранжевая книга»).	2					2
Тема 13. Концепция защиты АС и СВТ по руководящим документам Гостехкомиссии РФ.	2			5		7
Тема 14. Единые критерии безопасности информационных технологий (Common Criteria).	2	5	4	5		16
Подготовка к сдаче и сдача КП				19		19
Подготовка к сдаче и сдача экзамена					36	36
Всего в семестре	34	17	34	59	36	180
Итого по дисциплине	34	17	34	59	36	180

Интерактивные часы: 22 час.

6. Лабораторные занятия (работы)

Таблица 2.1 - Лабораторные по очной форме обучения

№ ЛЗ	Тема дисциплины	Тема и содержание ЛЗ	Кол-во часов ЛЗ
Семестр – 7 (17 час.).			
1.	Тема 4	Реализация политики информационной безопасности на примере дискреционной модели	4
2.	Тема 7	Изучение уязвимости модели Харрисона-Рузо-Ульмана	4
3.	Тема 8	Реализация распространения прав доступа по модели Take-grant	4
4.	Тема 14	Расширенная модель прав доступа Take-Grant	3
5.	Тема 14	Построение систем защиты с использованием модели контроля информационных потоков Белла-Лападуллы.	2
Итого по дисциплине			17

7. Практические занятия

Таблица 2.2 – Практические занятия по очной форме обучения

№ ПЗ	Тема дисциплины	Тема и содержание ПЗ	Кол-во часов ЛЗ
Семестр – 7 (34 час.).			
1.	Тема 8	Решетка многоуровневой безопасности.	2
2.	Тема 10	Расширенная модель Take-Grant. Правила де-юре и де-факто. Применение теоремы об условиях реализации информационного потока.	4
3.	Тема 10	Расширенная модель Take-Grant. Построение замыкания графа доступов.	4
4.	Тема 10	Модель ХРУ. Этапы обоснования теоремы об алгоритмической неразрешимости задачи проверки безопасности систем ХРУ.	4
5.	Тема 10	Сведение модели ХРУ к модели ТМД и наоборот. Сведение модели Take-Grant к моделям ХРУ и ТМД.	4

6.	Тема 10	Модель Белла-ЛаПадулы. Обоснование теоремы БТБ. Пример некорректной интерпретации свойств безопасности.	2
7.	Тема 10	Модель Белла-ЛаПадулы. Безопасность переходов.	2
8.	Тема 10	Модель СВС. Потенциальная модификация сущности.	2
9.	Тема 10	Модель СВС. Безопасная система. ss-, *-, ds-свойства безопасности.	2
10.	Тема 10	Модель мандатного ролевого управления доступом. Обоснование теоремы об информационных потоках. ss- и *-свойства безопасности.	2
11.	Тема 10	Анализ в рамках ДП-моделей информационных потоков по памяти или по времени.	2
12.	Тема 14	Подходы к классификации защищенности операционнных систем с использованием стандартов, руководящих документов Гостехкомиссии РФ и "Единых критериев"	4
Итого по дисциплине			34

8. Самостоятельная работа студента

Таблица 3 - Самостоятельная работа студента по очной форме обучения

№	Вид (содержание) СРС	Кол-во часов СРС	Форма контроля, аттестации
Семестр – 7 (68 час.)			
1.	Решение задач по модели TAM.	5	Текущий контроль: опрос, тест
2.	Решение задач TAKE-GRANT.	5	
3.	Решение задач по расширенной модели TAKE-GRANT.	5	
4.	Решение задач по модели Белла-ЛаПадуллы.	5	
5.	Решение задач по модели HRU.	5	
6.	Решение задач по модели тематического разграничения доступа на основе иерархических рубрикаторов. /Ср/	5	
7.	Решение задач по модели ролевого доступа при иерархически организованной системе ролей.	5	
8.	Решение задач по модели анализа индивидуально-групповых систем назначения доступа к иерархически организованным объектам доступа.	5	
9.	Подготовка к сдаче и сдача КП	19	
Всего за семестр:		59	
Итого по дисциплине		59	

9. Учебная литература и учебно-методическое обеспечение самостоятельной работы студента.

9.1. Основная учебная литература

1. Ищейнов, В. Я. Защита конфиденциальной информации : учеб. пособие / В. Я. Ищейнов, М. В. Мецатунян. – М. : ФОРУМ, 2013. – 256 с. (наличие в библиотеке БГАРФ - 15 экз.)
2. Шаньгин В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. – Электрон. текстовые дан. – Москва: ДМК Пресс, 2014. – 702 с. – Режим доступа: http://www.iprbookshop.ru/29257
3. Введение в информационную безопасность [Электронный ресурс]: учеб. пособие/ Малюк А. А. [и др.]. – Электрон. текстовые данные. – Москва: Горячая линия-Телеком, 2011. – 288 с. – Режим доступа: http://www.iprbookshop.ru/11979

9.2. Дополнительная учебная литература

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – М. : ИД «Форум», 2013. – 416 с. (наличие в библиотеке БГАРФ - 20 экз.)
2. Девянин, П. Н. Модели безопасности компьютерных систем : учебное пособие / П. Н. Девянин. - М. : Academia, 2005. - 144 с. - (Высшее профессиональное образование). - ISBN 5769520531 (39 экз.)
3. Кузнецов, А. В. Основы защиты информации : учеб. пособие / В. А. Иванов, О.П. Пономарев, И. А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 122 с. (наличие в библиотеке БГАРФ - 110 экз.)

9.3. Периодические издания

1. Защита информации. Инсайд : информационно-методический журнал. - СПб. : ООО "Изд. Дом "Афина".
2. Безопасность информационных технологий : научно-технический журнал. - М. : Изд-во журнала "Безопасность информационных технологий".

9.4 Учебно-методические пособия по дисциплине:

1. Подтопельный, Владислав Владимирович Теоретические основы компьютерной безопасности. Ч.1. [Электронный ресурс] : методические указания по выполнению лабораторных работ для студентов специальности 10.05.03 "Информационная безопасность автоматизированных систем" / В. В. Подтопельный, Н. Н. Смирнов ; БГАРФ ФГБОУ ВО "КГТУ". - 2-е изд., перераб. и доп. - Калининград : Издательство БГАРФ.

10. Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины.

Электронная информационная образовательная среда БГАРФ ФГБОУ ВО «КГТУ»: http://83.171.112.16/login/index.php

Программное обеспечение

Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription;

Номер контракта 0335100016118000073-0484577-02 от 05.07.2018

Kaspersky Total Space Security Russian Edition госконтракт № 13/18АВ от 23.01.2018 г

DALLAS LOCK 8.0-K

Договор о сотрудничестве

№ 252-18-ЦЗ/1

от 1.11.2018 г. (3 года)

СЗИ «Блокхост-МДЗ» Договор о со-трудничестве №012 от 14 июня 2018 г. (3 года)

Falcongaze SecureTower

Лицензионный договор №12/05/2018-1

от 05.12.2018 (1 год)

Интернет-ресурсы

Интернет-ресурсы, применяемые при изучении дисциплины:

Сайт ФСТЭК России.http://fstec.ru;

http://www.confident.ru;

http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/;

http://www.iqlib.ru - электронная интернет библиотека;

http://www.biblioclub.ru - полнотекстовая электронная библиотека;

http://www.elibrary.ru - научная электронная библиотека.

11. Материально-техническое обеспечение дисциплины

г. Калининград, ул. Молодежная 6, УК-1, ауд. 401 - учебная аудитория для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Специализированная (учебная) мебель - учебная доска, стол преподавателя, парты, стулья	
г. Калининград, ул. Молодёжная 6, УК-1, ауд. 250 – лаборатория специализации: обеспечение информационной безопасности распределённых информационных систем	12 компьютеров, Интернет Столы компьютерные – 12 шт. доска меловая – 1 шт. Стол преподавателя – 1 шт. Парта – 1 шт. Стулья – 15 шт.	Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription; Номер контракта 0335100016118000073-0484577-02 от 05.07.2018 Kaspersky Total Space Security Russian Edition госконтракт № 13/18АВ от 23.01.2018 г DALLAS LOCK 8.0-K Договор о сотрудничестве № 252-18-ЦЗ/1 от 1.11.2018 г. (3 года) СЗИ «Блокхост-МДЗ» Договор о сотрудничестве №012 от 14 июня 2018 г. (3 года) Falcongaze SecureTower Лицензионный договор №12/05/2018-1 от 05.12.2018 (1 год)
г. Калининград, ул.Молодёжная 6, УК-1, ауд. 437- кабинет курсового, дипломного проектирования, НИР	Специализированная (учебная) мебель: - 2 компьютера с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду организации, комплект лицензионного программного обеспечения, - оборудование для печати (2 шт.) - информационная доска, - компьютерные столы (2 шт) -учебные столы (6) -шкаф (3 шт.)	Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription; Номер контракта 0335100016118000073-0484577-02 от 05.07.2018 Kaspersky Total Space Security Russian Edition госконтракт № 13/18АВ от 23.01.2018 г DALLAS LOCK 8.0-K Договор о сотрудничестве № 252-18-ЦЗ/1

		от 1.11.2018 г. (3 года) СЗИ «Блокхост-МДЗ» Договор о сотрудничестве №012 от 14 июня 2018 г. (3 года) Falcongaze SecureTower Лицензионный договор №12/05/2018-1 от 05.12.2018 (1 год)
г. Калининград, ул. Молодёжная 6, УК-1, ауд. 431 (1)- кабинет для самостоятельной работы	Специализированная (учебная) мебель: - 2 компьютера с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду организации, комплект лицензионного программного обеспечения, - информационная доска, -учебные столы (7 шт.) -шкаф (1 шт.)	Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription; Номер контракта 0335100016118000073-0484577-02 от 05.07.2018 Kaspersky Total Space Security Russian Edition госконтракт № 13/18АВ от 23.01.2018 г

12. Фонд оценочных средств для проведения аттестации по дисциплине.

Аттестация по дисциплине (итоговая аттестация по дисциплине является промежуточной аттестацией по образовательной программе). Для рабочей программы разработано и утверждено приложение «Фонд оценочных средств для аттестации по дисциплине «Теоретические основы компьютерной безопасности».

13. Особенности преподавания и освоения дисциплины

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

13.1 Под образовательными технологиями будем понимать пути и способы формирования компетенций. В рамках дисциплины предусмотрены:

- лекции;
- лабораторные занятия, во время которых отрабатываются практические навыки по дисциплине, обсуждаются вопросы лекций, т.д.;
-практические занятия, во время которых решаются типовые задачи исследования моделей безопасности компьютерных систем.
- самостоятельная работа студентов, включающая усвоение теоретического материала, подготовку к практическим занятиям, выполнение индивидуальных заданий, курсового проекта, работа с учебниками, иной учебной и учебно-методической литературой, подготовка к текущему контролю успеваемости, к экзамену;
- тестирование по отдельным темам дисциплины;
- консультирование студентов по вопросам учебного материала.

13.2 Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение лабораторных занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

14. Методические указания по освоению дисциплины

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста):
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники:
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы:
- решить предложенные задачи, кейсы, ситуации;
- выполнить курсовой проект .

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам:
2. Выполнение курсового проекта;
3. Подготовка и сдача курсового проекта, итоговых экзаменов:

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) - важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение курсового проекта;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента *не* регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

• чтение текста (учебника, первоисточника, дополнительной литературы);

• составление плана текста;

• конспектирование текста;

• выписки из текста;

• работа со словарями и справочниками;

• исследовательская работа;

• использование аудио- и видеозаписи;

• работа с электронными информационными ресурсами и ресурсами Internet:

Для закрепления и систематизации знании:

• работа с конспектом лекции (обработка текста);

• повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио-видеозаписей):

• составление плана и тезисов ответа;

• выполнение тестовых заданий;

• ответы на контрольные вопросы;

• аннотирование, реферирование, рецензирование текста;

• подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;

• работа с компьютерными программами;

• подготовка к сдаче экзамена;

Для формирования умений:

• решение задач и упражнений по образцу;

• решение вариативных задач и упражнений:

• решение ситуационных производственных (профессиональных) задач;

• участие в научных и практических конференциях;

• проектирование и моделирование разных видов и компонентов профессиональной деятельности;

• создание проспектов, проектов, моделей;

• экспериментальная работа, участие в НИР;

• рефлексивный анализ профессиональных умений с использованием аудио-видеотехники и компьютерных расчетных программ и электронных практикумов;

• подготовка курсового проекта;

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Рабочая программа дисциплины «Теоретические основы компьютерной безопасности» представляет собой компонент образовательной программы специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализации «Обеспечение информационной безопасности распределенных информационных систем» и соответствует учебному плану, утвержденному 31 января 2018 г. и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор программы – к.ф.-м.н. Великите Н.Я.

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры «Информационная безопасность»
(протокол № 9 от 14 июня 2018 г.)

Заведующий кафедрой _____ /Н.Я. Великите/

Рабочая программа дисциплины рассмотрена и одобрена на заседании методической комиссии Совета РТФ

(протокол № 9 от 27 июня 2018 г.)

Председатель методической комиссии _____ /А.Г. Жестовский/